

全千兆 QoS 安全路由器

具负载均衡，带宽管理，网络安全等功能

简体中文使用手册

目錄

产品功能说明手册使用许可协议

《产品功能说明手册（以下称”手册”）使用许可协议》（以下称”协议”）是用户与侠诺科技股份有限公司（以下称”侠诺”）关于手册许可使用及相关方面的权利义务、以及免除或者限制侠诺责任的免责条款。直接或间接取得本手册档案以及享有相关服务的用户，都必须遵守此协议。

重要须知：侠诺在此提醒用户在下载、阅读手册前阅读本《协议》中各条款。请您审阅并选择接受或不接受本《协议》。除非您接受本《协议》条款，否则请您退回本手册及其相关服务。您的下载、阅读等使用行为将视为对本《协议》的接受，并同意接受本《协议》各项条款的约束。

【1】知识产权声明
手册内任何文字表述及其组合、图标、界面设计、印刷材料、或电子文件等均受我国著作权法和国际著作权条约以及其它知识产权法律法规的保护。当用户复制"手册"时，也必须复制并标示此知识产权声明。否则，侠诺视其为侵权行为，将适时予以依法追究。

【2】"手册"授权范围：
用户可以在配套使用的计算机上安装、使用、显示、阅读本"手册"。

【3】用户使用须知
用户在遵守法律及本协议的前提下可依本《协议》使用本"手册"。本手册"纸质或电子档案"，仅限于为信息和非商业或个人之目的使用，并且不得在任何网络计算机上复制或公布，也不得在任何媒体上传播;及不得对任何"档案"作任何修改。为任何其它目的之使用,均被法律明确禁止,并可导致严重的民事及刑事处罚。违反者将在可能的最大程度上受到指控。

【4】法律责任与免责声明
【4-1】侠诺将全力检查文字及图片中的错误，但对于可能出现的疏漏，用户或相关人士因此而遭受的直接或间接的经济损失、数据损毁或其它连带的商业损失，侠诺及其经销商与供货商不承担任何责任。
【4-2】侠诺为了保障公司业务发展和调整的自主权，侠诺拥有随时自行修改或中断软件 / 手册授权而不需通知用户的权利，产品升级或技术规格如有变化，恕不另行通知，如有必要，修改或中断会以通告形式公布于侠诺网站的相关版块。
【4-3】所有设置参数均为范例，仅供参考，您也可以对本手册提出意见或建议，我们会参考并在下一版本作出修正。
【4-4】本手册为解说同系列产品所有的功能设置方式，产品功能会按实际机种型号不同而有部份差异，因此部分功能可能不会出现在您所购买的产品上。

【4-5】侠诺保留此手册档案内容的修改权利，并且可能不会实时更新手册内容，欲进一步了解产品相关更新讯息，请至侠诺官方网站浏览。

【4-6】侠诺（和/或）其各供货商特此声明，对所有与该信息有关的保证和条件不负任何责任，该保证和条件包括关于适销性、符合特定用途、所有权和非侵权的所有默示保证和条件。所提到的真实公司和产品的名称可能是其各自所有者的商标，侠诺（和/或）其各供货商不提供其它公司之产品或软件等。在任何情况下,在由于使用或档案上的信息所引起的或与该使用或运行有关的诉讼中, 侠诺和/或其各供货商就因丧失使用、数据或利润所导致的任何特别的、间接的或衍生性的损失或任何种类的损失，均不负任何责任，无论该诉讼是合同之诉、疏忽或其它侵权行为之诉。

【5】其它条款

【5-1】本协议高于任何其它口头的说明或书面纪录，所定的任何条款的部分或全部无效者，不影响其它条款的效力。

【5-2】本协议的解释、效力及纠纷的解决，适用于台湾法律。若用户和侠诺之间发生任何纠纷或争议，首先应友好协商解决。若协商未果，用户在完全同意将纠纷或争议提交侠诺所在地法院管辖。中国则以「中国国际经济贸易仲裁委员会」为仲裁机构。

一、简介

全千兆 QoS 安全路由器是因应高效能路由器市场需求，为满足中大型网咖、企业与小区等宽带应用高的大型网络环境，所设计的高效能、全功能的网络安全路由器。并针对多个运营商环境及用户带宽管理需求，结合全千兆骨干组网方案，支持硬件镜像端口、智能型带宽管理、多 WAN 负载均衡、线路备援、强效防火墙等功能。

此路由器采用 64 位多核心硬件加速高阶网络专用处理器，双向转发速率 2Gbps，可支持 120,000 联机数，封包处理快速稳定。内建高规格大容量内存，长时间高负载运作稳定可靠。

具备 3~4 个全千兆 WAN 端口，并具有高效能线路负载平衡模式的功能，达到对外联机的流量负载平衡。WAN 端的对外联机能力满足绝大多数宽带市场都适用的规格。此外，DMZ 端口可以连接具有公网 IP 地址的对外服务器。区域网端内建 1~2 个全千兆骨干 LAN 端口，Auto-MDI/MDI-X 10/100/1000Mbps 以太网络交换器，每个埠都可以连接额外的交换器以连接更多的上网设备，方便建立千兆骨干，加速企业网络效能，带宽成长空间大。提供硬件 USB 人性化接口，将来可以外接支持 USB 相关的装置，扩充功能或数据储存容量等。

独特的 QoS 带宽管理功能，功能强大但是设定简单，可以让管理者对有限的网络资源做合理而且有效的分配。对外不需要无限制的扩充带宽而花费过多的金钱，也不会因为少数几人的下载而强占所有的带宽，造成内部的抱怨。简化了用户设置，不需要一一设规则，即可依整体使用情况，优化带宽利用，并只针对大量占用者加以限制，节省运算资源，可达成最有效率的运用。同时提供智慧带宽管理，通过简单的设置完成内网带宽管理，达到有效率的带宽使用，简化管理，提高工作效率。

本系列路由器更具备了独家的硬件加速服务，将带宽管理、优化流量使用分配等相关动作，直接以硬件执行，除了可达到保障并加速内网的重要服务流量的使用，即使是在带宽全部满载的状况下，仍然可以顺畅的使用这些重要的服务不会中断；更可以大幅减少 CPU 与整体系统资源的消耗，使路由器更能承受庞大的联机数量与计算机数量，提供绝佳且稳定的网络使用环境。

负载均衡模式支持智能线路、IP 地址、策略路由三种带宽均衡模式，提供弹性灵活的网络联机需求设置，来进行流量的负载均衡控制，可保证所有线路畅通。策略路由设置简化无需导入 IP 地址文件，自动判别对外网络数据报，分流电信网通线路，确保跨网联机反应快速、通行无碍，可汇聚不同运营商的线路带宽，作负载均衡控制，大大提升网络资源运用的灵活度。

强效的防火墙系统，以满足多数企业对防御外部网络攻击的市场需求。主动式封包检测功能，经由对网络层联机的动态检测，拒绝或阻挡非标准通信协议的联机要求。只需单向启动各式黑客攻击、蠕虫病毒、ARP 攻击防护功能，即可简易完成配置，有效防止内外网恶意攻击，确保网络安全。防火墙系统除了 NAT 之外，还具备有防止阻断服务攻击。功能完整的存取规则设定，可让管理者选择应该禁止或开放存取的网络服务，限制或禁止区域网内用户的网络权限，以避免占用网络资源或是不当使用而遭受潜在的危机。

网络地址转换(NAT) 除了可以做私网与公网的 IP 转换，让您只需要一个公网 IP 就可以让多人同时连上网络。区域网内的 IP 地址支持 4 个 Class C 等级，DHCP 自动分配 IP，以及简单勾选的 IP 与 MAC 地址绑定让网络环境架构具有弹性，易于规划管理。

此外，本路由器还具有虚拟路由功能，单线分点轻松晋级享有双线传输，只有单线的企业分点通过设定联机至具有双线的中心端，通过中心点转发到另一条线路出去，加速跨越不同运营商的联机问题。

此说明书主要是用来说明每一个功能的设定方法与细节，若是您对于路由器如何连上网络的设定并不十分清楚，建议您先阅读“快速安装说明”，可以让您快速的将路由器连上网络，并在必要时取得技术人员的远程支持。

您可上网 www.Qno.cn 进行在线登录，以取得最新侠诺产品信息及应用实例，更加善用您的侠诺产品。

此为 FCC Class A 级产品，在生活环境中该产品可能会造成无线电干扰，在这种情况下可能需要使用者对其干扰采取确实可行措施。

二、安全路由器设置操作流程

本章节介绍用户整体设置安全路由器操作流程，通过对安全路由器多 WAN 设置流程的了解可以很轻松的设置我们的网络，来有效的管理我们的网络，使安全路由器达到应有的功能，使安全路由器的效能达到最高。

2.1 系统性设置流程的需要

用户可以通过以下操作流程设置网络，能够使网络有效利用带宽，网络效能达到理想的效果，同时可以阻断一些攻击与预防一些安全隐患，通过流程设置更加方便用户的安装与操作，简化维护管理的难度，使得用户的网络设置一次到位。设置主要流程如下：

1、 硬件安装。

2、 登录设置窗口。

3、 确定设备规格及进行密码和时间设置。

4、 进行广域网联机的设置：进行内部联机的设置。

5、 进行局域网联机的设置：实体线路设置及 IP 地址设置

6、 进行 QoS 带宽管理设置：防止带宽占用情况。

7、 进行防火墙设置：预防攻击及不当存取网络资源。

8、 其它特别设置：开放服务器、UPnP、DDNS、MAC 克隆。

9、 管理维护的设置系统日志、SNMP、及设置参数备份注销设置窗口。

10、 注销设置窗口

2.2 设置流程表

下表主要阐述每个设置流程相对应的安全路由器管理内容以及此设置所达到的目的，如需详细了解每步过程以及后面章节介绍所对应的内容，可参考（附录一、设置界面及使用手册章节对照）。

#	设置	内容	目的
1	硬件安装	构建用户需要的网络	根据用户实地网络的要求来安安全路由器硬件。
2	登录设置窗口	从计算器 Web 接入安全路由器设置窗口，了解系统信息	登录安全路由器的 Web 管理页面。

3	确定设备规格	确定产品软件版本以及路由工作情况	确定安全路由器规格，系统软件版本，以及安全路由器工作状况。
	进行密码及时间设置	设置时间及修改密码	安全的考虑修改登录密码。 设置安全路由器时间与广域网络同步。
4	进行广域网联机的设置	确定广域网线路设置、带宽调配、及协议绑定	连接广域网络，通过带宽的设置等能更好的利用带宽，优化数据转发能力。
5	进行局域网联机的设置：实体线路设置及 IP 地址设置	端口镜像及 VLAN 设置。内部用户 IP 的分配群组及管理	应地区需求提供端口镜像功能，同时改进端口管理及 VLAN 的设置满足内网相关需求，弹性提供固定 IP/DHCP 自动 IP 地址分配，方便用户在不同网络环境的需要。IP 群组管理对一组 IP 地址做相同设置，简化管理工作。
6	进行 QoS 带宽管理设置，防止带宽占用情况的发生	广域网端口、内部用户或应用流量及联机数的限制	确保网络重要信息不致延迟、确保网络重要应用服务联机顺畅；进一步针对现有的带宽进行管理运用，让有限的带宽资源发挥最大的效用。
7	进行防火墙设置，预防攻击及非法访问网络资源	攻击阻挡、访问规则及网页存取限制	当内网用户使用 BT、点点通影响其它人上网、员工上班时间不正当上网以及使用 MSN、QQ、Skype 影响工作效率；当网速因被黑客攻击而受影响或内网用户常被蠕虫及 ARP 软件所苦；网管可依据需求设置内外网络存取规则，以进一步管控员工个别上网行为。
8	其它特别设置：开放服务器、UPnP、DDNS、MAC 克隆	针对内部设置开放服务器、UPnP、路由模式、多广域网 IP、DDNS、Mac 克隆	高级管理设置完成对网络的更高一步要求，构建内部开放服务器，虚拟服务器，UPnP 通讯协议的设置，设置动态路由或者静态路由，一对一 NAT 设置，动态域名解析服务与 Mac 地址克隆。
9	管理维护的设置：系统日志、SNMP、及设置参数备份	安全路由器工作情况监测、系统参数的备份	网管可借此功能查看系统日志、即时监控系统状态及内外流量，确保内网运作无误。
10	注销设置窗口	离开设置窗口	注销退出安全路由器 Web 管理页面。

下面我们就根据这个流程来设置完成我们的网络设置。

三、硬件安装

本章介绍产品的硬件接口以及实体安装。

3.1 安全路由器 LED 显示灯

LED 灯号说明

LED	颜色	意义
Power-电源	绿灯	绿灯亮： 电源开启连接
DIAG-自我测试	橘灯	橘灯亮： 系统尚未完成开机自我检测功能。 橘灯熄灭： 系统已经正常完成开机自我检测功能。
Link/Act-联机/动作 （端口右侧绿灯）	绿灯	绿灯亮： 以太网络联机正常 绿灯闪烁： 以太网络端口正在传送/接收数据包数据传输
10M/100M/1000M-速度 （端口左侧灯）	橘灯	橘灯熄灭： 以太网络联机在 10Mbps 的速度 橘灯亮： 以太网络联机在 100Mbps 的速度 绿灯亮： 以太网络联机在 1000Mbps 的速度
USB(未来支持)	绿灯	绿灯亮：USB 已连接且设备有支持 绿灯闪烁：USB 端口正在传送/接收封包数据传输

硬件恢复 (Reset) 按键

动作	意义
点击 Reset 按钮 5 秒	热开机，重新启动安全路由器 DIAG 灯号： 橘色灯号慢慢闪烁
点击 Reset 按钮 10 秒以上	恢复原出厂默认值 DIAG 灯号： 橘色灯号快闪

系统内建电池

安全路由器内建有系统时间的电池，此电池的寿命约为 1～2 年，当电池已经无法充电或是使用寿命到达后，安全路由器将无法记录时间或是连接互联网同步 NTP 时间服务器。您必须与您的供应商联系，以便取得更换电池技术。

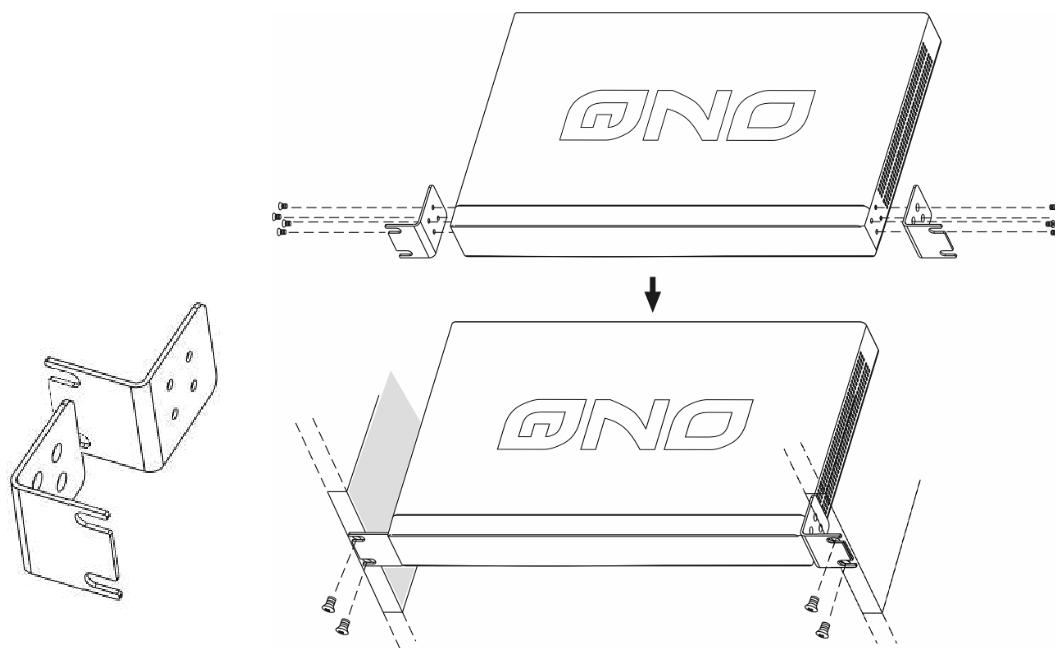
> 注意！
> 为了产品的正常运行，请勿自行更换电池，以免造成产品无法恢复的损坏！

将安全路由器安装在 19”标准机架上

建议您可以将安全路由器放置于桌上使用，或是您有机房专用 19 吋标准机架的话，可以将安全路由器安装于机架上，每一台安全路由器都有配备专用连接机架配件。当您安装安全路由器于机架上的时候，请注意不要将其它过重的物品堆栈或是放置于机器上，以免因无法负重而发生危险或是损伤机器本体。

每一台安全路由器都有配备专用连接机架配件，包含 2 只 L 型锁附架以及八颗专用螺丝，用来将安全路由器安

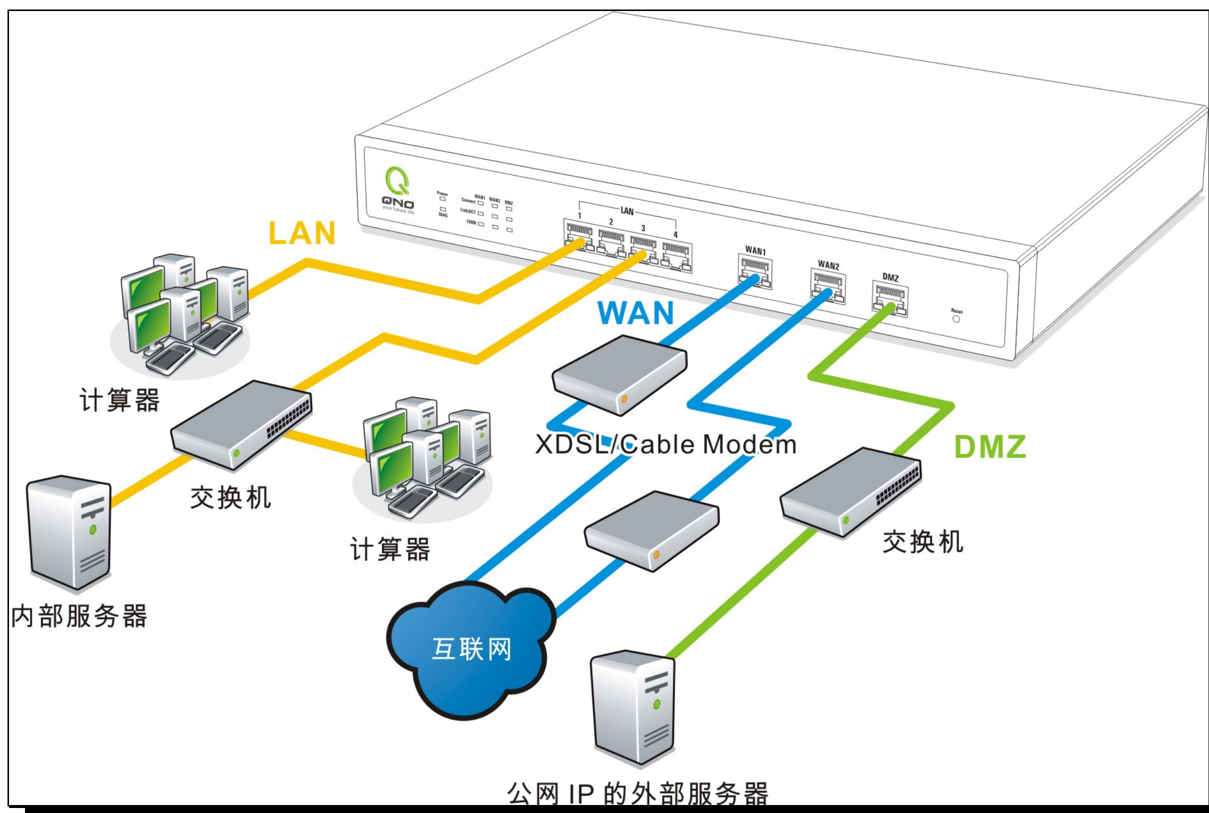
装在机架上使用。安装于您的 19 吋标准机架上的方法如下图所示：



注意！

为了产品的稳定运行，无论您是如何放置安全路由器，请不要阻塞产品两侧通风口的任何一侧，并保持通风口有 10 厘米以上的通风空间！

3.2 安全路由器的网络连接



广域网络联机：连接 xDSL Modem 或光纤盒来连通互联网。或是连接交换机或外部路由器、防火墙来连通您现有的网络。

局域网络联机：连接交换机或计算机。若局域网端口有支持镜像功能，请在“端口管理”中做设置，设定完成即可直接将监控或过滤服务器接在此端口使用

DMZ 端口：此端口可以连接如 Switch HUB 或是具有外部合法 IP 地址的服务器，如网页服务器以及电子邮件服务器等。

四、登录安全路由器

本章主要是在客户连接好安全路由器后，通过连接安全路由器的计算机登录安全路由器的 Web 管理页。

首先在连接到安全路由器 LAN 端的计算机（确定计算机是自动获得 IP 地址）上的 DoS 下查找安全路由器的 IP 地址，点开始→运行，输入“cmd”命令进入 DoS 操作，再输入“ipconfig”命令→确认，查到默认网关（Default Gateway）地址如图，192.168.1.1。确认默认网关也就是安全路由器的默认 IP 地址。

```
C:\WINDOWS\system32\CMD.exe
Microsoft Windows XP [版本 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\PM01>ipconfig

Windows IP Configuration


Ethernet adapter 區域連線:

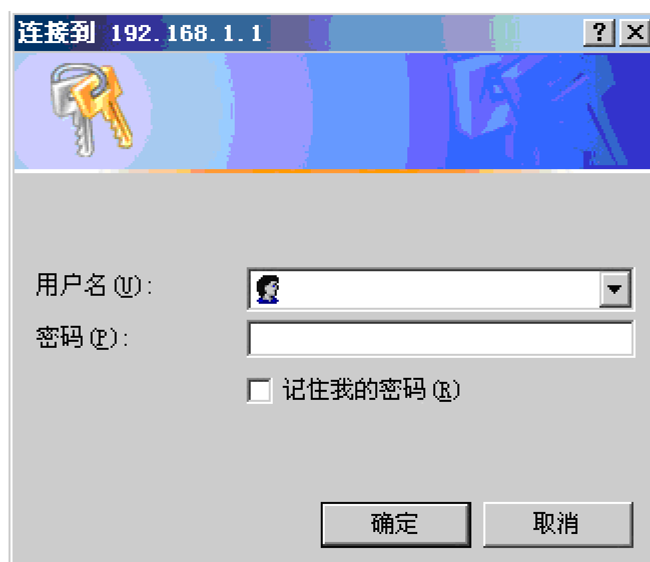
        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 192.168.1.100
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.1.1

C:\Documents and Settings\PM01>_
```

注意！

当“ipconfig”不能获得 IP 地址以及默认网关的情况，或者获得的 IP 地址为 0.0.0.0 以及 169.X.X.X 的情况，就是安全路由器并没有分配到 IP 地址，建议用户检查线路是否有问题，计算机网卡是否接好等。

然后开启网页浏览器 (如 IE)，在网址栏输入 192.168.1.1 (安全路由器的默认网关)，会出现以下的登录窗口：



安全路由器默认的使用者名称(User Name)与使用者密码(Password)皆为“admin”，您可以在进入路由管理页面后）更改此用户名及登录密码。

注意！

为了安全，我们强烈建议您务必在登录之后更改管理密码！密码请牢记，若是密码忘记，将无法再登录至安全路由器的设置窗口，必须点击面板上的 Reset 按键十秒以上，恢复到出厂值，其所有设置将需要重新设置。

登录后，就会显示安全路由器的 Web 管理页面，在其页面的右上角选择安全路由器操作的语言模式，选中的图标将变成蓝色，这里选择“简体”（简体中文版本），如图。



五、确定设备规格、状态显示以及登录密码和时间的设置

本章介绍登录软件设置窗口后，进入首页可以了解到的设备规格以及设备工作状态信息，还有因安全考虑需要用户即时修改登录密码与系统时间设置。

5.1 首页显示

首页显示安全路由器目前系统所有参数以及状态显示信息。

5.1.1 系统信息

广域网状态

接口位置	广域网2	广域网1	USB
IP地址	220.130.188.40	0.0.0.0	---
默认网关	220.130.188.33	0.0.0.0	---
DNS 服务器	168.95.1.1 0.0.0.0	0.0.0.0	---
会话数	3	0	---
下载带宽使用率(%)	0	0	---
上传带宽使用率(%)	0	0	---
动态域名服务	Dyndns 关闭 3322 关闭 Qnoddns 关闭	Dyndns 关闭 3322 关闭 Qnoddns 关闭	Dyndns 关闭 3322 关闭 Qnoddns 关闭
QoS带宽管理	0 条规则	0 条规则	---
手动连接	释放 更新	释放 更新	释放 更新

*此为示意图，会因产品线不同，图形会有所差异

IP 地址： 此为显示安全路由器 WAN 端目前的 IP 地址信息。

默认网关： 此为显示运营商分配给安全路由器 WAN 的网关 IP 地址信息。

DNS 服务器： 此为显示安全路由器的 DNS 的 IP 地址信息。

会话数： 此为显示安全路由器每个 WAN 目前的会话数目。

下载带宽使用率： 此为显示安全路由器每个 WAN 目前的下载带宽使用比例。

上传带宽使用率： 此为显示安全路由器每个 WAN 目前的上传带宽使用比例。

动态域名服务： 此为显示安全路由器的 DDNS 是否启动的状态信息。系统默认此功能为关闭。

QoS 带宽管理： 此为显示安全路由器的网络质量服务(QoS)是否开启。

手动连接： 当使用者选择自动取得 IP 地址时，他会显示二个按钮分别为释放与更新。使用者可以点击释放按钮去做释放运营商端所核发的 IP 地址，以及点击更新按钮去做更新运营商端所核发的 IP 地址。

当选择 WAN 端联机使用如 PPPoE 或是 PPTP 的话，它会变为显示“连接”与“中断”。

5.1.2 硬件端口状态实时显示

端口配置状态

端口号	1	2	3	4
接口位置	局域网			
状态	激活	激活	激活	激活

端口号	Internet	Internet
接口位置	广域网1	广域网2
状态	连接	激活

*此为示意图，会因产品线不同，图形会有所差异

此窗口会显示系统各端口目前实时状态：(连接-已经连接，激活-此端口处于开启状态，关闭-此端口处于关闭状态)。您可以点击此状态按钮，在弹出的窗口中查看各端口更详细的资料显示。如下图：

广域网1 信息

摘要信息：

网路连接状态	10Base-T / 100Base-TX / 1000Base-T
接口位置	广域网1
线路连线状态	激活
端口配置状态	端口激活
优先级设定	一般
连接速率	100 Mbps
半双/全双工模式	全双工
自动翻转功能	激活

流量实时状态：

接收数据包统计	0
数据包接收Byte数量	107885800
传送数据包统计	0
数据包传送Byte数量	65509869
错误数据包统计	0

刷新 关闭

此表会显示目前该端口设置状态，如网路连接状态(10Base-T/100Base-TX/1000Base-T)，接口位置(广域网／局域网/DMZ)，线路连接状态(激活/关闭)，端口设置状态(端口激活/端口关闭)，优先级设置(高级/一般)，网络连接速率(10Base-T/100Base-TX/1000Base-T)，工作模式(半双工/全双工)，以太网自动翻转功能(激活/关闭)。于此项目表格中，会显示此端口的接收和传送的数据包以及数据包传送 Byte 数及数据包错误率等并计算总数量。

5.1.3 系统信息

系统信息

局域网网关/子网掩码	10.10.10.1/255.255.255.0
工作模式	NAT模式
运作时间	7天 7时 10分 25秒

序列号	
软件版本	2.1.0.1-Qno (Jun 26 2008 20:38:08)
当前时间	Fri Jul 4 2008 18:21:06

局域网网关地址： 此为显示安全路由器 P 本身的 LAN 端目前 IP 地址，系统默认为 192.168.1.1。

工作模式： 此为显示安全路由器的目前工作模式(可为 NAT 模式或是路由模式)。

系统默认此功能为 NAT 模式。

运作时间：此为显示安全路由器目前已经开机的时间。

主机序列号：此为显示安全路由器的产品序号。

软件版本： 此为显示安全路由器 目前使用的硬件版本。

当前时间：此显示安全路由器 目前正确时间，但必须注意，您需要正确设置与远程 NTP 服务器的时间同步后才会正确显示。

5.1.4 防火墙状态

防火墙状态

防火墙	状态
SPI数据包检测	激活
防止DoS攻击功能	激活
阻止广域网回应功能	关闭
防止ARP病毒攻击	关闭
远程管理功能	激活
访问规则设置	7 条规则

SPI 数据包检测：此为显示安全路由器的 SPI 主动数据包侦测过滤功能选项是否激活(激活/关闭)。

系统默认此功能为激活。

防止 DoS 攻击功能：此为显示安全路由器的阻断来自网络上的 DoS 攻击功能选项是否开启(激活/关闭)。

系统默认此功能为激活。

阻止广域网回应功能：此为显示安全路由器的阻断来自网络上的 ICMP-Ping 的响应功能选项是否激活(激活/关闭)。系统默认此功能为激活。

防止 ARP 病毒攻击：此为显示安全路由器防止 ARP 攻击的功能选项是否激活(激活/关闭)。

系统默认此功能为关闭。

远程管理功能：此为显示安全路由器的远程管理功能选项是否启动(激活/关闭)。系统默认此功能为关闭。

访问规则设置： 此为显示安全路由器的访问规则设置的数目。

5.1.5 系统日志设置状态显示

系统日志配置状态

发送到日志服务器	关闭
发送到电子邮箱	关闭

发送到日志服务器： 此为显示您所设置安全路由器日志记录接收的服务器。

发送到电子邮箱： (未来支持) 此为显示您所设置的 E-mail 地址，安全路由器的日志记录经由此 E-mail 传送出去。

E-Mail 的链结将会连到系统日志设定窗口中：

1. 若您没有设定电子邮件服务器于系统日志设定中，将显示 "**邮件无法传送，因为没有配置 SMTP 服务器正确地址**"——表示您没设定电子邮件服务器所以无法发送系统日志电子邮件。

2. 若您已经设定电子邮件服务器于系统日志设定中，但是日志尚未达到设定传送的条件时，将显示"**邮件设定已经配置**"——表示您的电子邮件服务器已经设置，但是日志尚未达到设定传送的条件时。

3. 若您已经设定电子邮件服务器于系统日志设定中，日志也已经传送出去时，它将显示 "**邮件设定已经配置并正常发送**"——表示您的电子邮件服务器已经设置，并且已经发送。

4. 若您已经设定电子邮件服务器于系统日志设定中， 但是日志无法正确传送出去时，它将显示 "**邮件不能发送，请使用正确的配置**"——电子邮件服务器已经设置，但是无法传送出去，可能是设定有问题。

5.2 登录密码及时间的修改和设置

5.2.1 密码设置

当您每次登录安全路由器的设置窗口时，必须输入密码。安全路由器的用户名和密码出厂值均为"admin"。考虑安全因素，我们强烈建议您务必在第一次登录并完成设置之后更改管理密码！密码请牢记，若是密码忘记，将无法再登录安全路由器的设置窗口，必须点击安全路由器前面板上的 Reset 按键十秒以上，恢复到出厂值，所有设置值将需要重新设置。

密码设置

用户名：	admin
密码：	
更改用户名：	admin
输入新密码：	
再次输入新密码：	

确定 取消

用户名： 出厂初始值默认为 admin。

密码： 填写原本旧密码（出厂初始值默认为"admin"）。

更改用户名： 输入新用户名，如 Qno。

输入新密码： 填写要更改的新密码。

再次输入新密码： 再次填写更改的新密码以确认。

确定： 点击此按钮"确定"存储刚才所修改设置的内容参数。

取消： 点击此按钮"取消"清除刚才所修改设置的内容参数，此操作必须于"确定" 存储动作之前才会有效。

5.2.2 系统时间设置

安全路由器可以设置时间，让您在查看安全路由器的系统纪录或设置网络存取的时间设置时，可以了解事件发生的正确时间，以及作为关闭存取或是开放存取网络资源的依据条件。您可以选择与安全路由器内建的外部时间服务器(NTP 服务器)取得时间同步，或自己设置正确时间参数。

与外部时间服务器同步：安全路由器有内建的网络时间服务器，会自动同步时间。

◉ 与外部时间服务器同步
○ 手动配置时间

时区选择：	Hong Kong (GMT+08:00)
夏令时：	☑ 激活 从 3 月 28 日 到 10 月 28 日
外部时间服务器地址：	

确定 取消

时区选择： 点开下拉菜单选择您所在地点的时区以正确显示当地时间。

夏令时： 若是您所的地区有实施日光节约时间，可以输入实施的日期范围，安全路由器会在此日期范围自动调整时间。

外部时间服务器地址： 若是您自己有偏爱使用的时间服务器，可以输入该服务器的地址。

确定： 点击此按钮即会存储刚才所变动的修改设置内容参数。

取消： 点击此按钮即会清除刚才所变动的修改设置内容参数，此操作必须于确认存储动作之前才会有效。

手动设置时间： 在这输入正确的时间：小时、分钟、秒、月份、日与年份。

○ 与外部时间服务器同步
◉ 手动配置时间

19 时 7 分钟 1 秒
7 月 4 日 2008 年

确定 取消

点击“确认”按钮即会存储刚才所修改的设置内容参数，点击此按钮“取消”即会清除刚才所修改的设置内容参数，此操作必须于确认存储动作之前才会有效。

六、广域网络连线设置

本章节讲述基本的广域网络设置，对大多数的用户来说，通过本章节完成基本的设置已经足够连接网络。网络的连接需要一些运营商所提供的进一步详细信息。其详细项目设置，请参考以下各节说明：

6.1 网络设置

主机名称：	(某些 ISP 要求输入)
网域名称：	(某些 ISP 要求输入)

局域网(LAN)接口配置

MAC 地址设定 00 - 17 - 16 - 99 - 45 - 20 (预设值:00-17-16-99-45-20)	
IP 地址 ：192.168.0.1	子网掩码 ：255.255.252.0
多重网段配置	关闭

IP 整合管理

连线类型配置

端口	线路连线类型	配置
广域网1界面	PPPoE 设定（ADSL拨号使用者）	编辑
广域网2界面	PPPoE 设定（ADSL拨号使用者）	编辑

激活此选项会设定 DMZ 端口

确定 取消

*此为示意图，会因产品线不同，图形会有所差异

6.1.1 主机名称及域名

主机名称	SMB	(某些ISP要求输入)
网域名称	smb.com	(某些ISP要求输入)

可输入安全路由器的名称（主机名称）以及网域名称，此设置在大多数环境中不需要做任何设置即可使用，除非特殊运营商需求！

6.1.2 局域网（LAN）接口设置

此为设置安全路由器的 LAN 端内部网络的 IP 地址，系统默认为 192.168.1.1，子网掩码为 255.255.255.0，您可以依照实际网络架构做变动。

局域网(LAN)接口配置

MAC 地址设定 00 - 17 - 16 - 99 - 45 - 20 (预设值:00-17-16-99-45-20)	
IP 地址 : 192.168.0.1	子网掩码 : 255.255.252.0
多重网段配置	关闭

IP 整合管理

IP 整合管理：

IP 整合管理的设置窗口可以设定局域网(LAN) IP、动态 IP(DHCP)发放范围。

Unified IP Management - Windows Internet Explorer

http://61.222.81.94/ip_management.htm

區域網路(LAN)設定

設備IP位址 192 . 168 . 1 . 1	子網路遮罩 255 . 255 . 255 . 0

多個子網設定 ☐ 多個子網

區域網路IP位址

子網路遮罩

增加到對應表列

刪除選中的子網

動態IP

☑ 啟用DHCP伺服器

	子網域1	子網域2	子網域3	子網域4
DHCP伺服器	☑ 啟用	☐ 啟用	☐ 啟用	☐ 啟用
起始IP位址	192 . 168 . 1 . 100	192 . 168 . 2 . 100	192 . 168 . 3 . 100	192 . 168 . 4 . 100
終止IP位址	192 . 168 . 1 . 149	192 . 168 . 2 . 149	192 . 168 . 3 . 149	192 . 168 . 4 . 149

完成 網際網路 | 受保護模式: 關閉 100%

区域网络(LAN)设定：

系统默认 LAN IP 为 192.168.1.1，子网掩码为 255.255.255.0，您可以依照实际网络架构做变动。

Multiple-Subnet 多子网配置：

勾选“多个子网”，并填入您想要增加的子网 IP 地址以及子网掩码，即可增加新的子网在局域网。此功能是将不同于路由器局域网段的其他网段 IP 加入到路由器认可的局域网段中，这样局域网中的 PC 若是已经设定的 IP 所在的网段不同于路由器的局域网段也可以直接上网。举例来说，原来内部环境已经有多组不同的 IP 网段，例如 192.168.3.0， 192.168.20.0， 192.168.150.0 等等，将这些网段加入到子网中，则这些网段的内部计算机不需做任何修改就可以上网，这里可以依照您的实际网络架构运作。

动态 IP：

路由器有四组 Class C 的 DHCP 服务器，默认值是激活，可以提供局域网络内的计算机自动取得 IP 的功能，(如同 NT 服务器中的 DHCP 服务)，好处是每台 PC 不用去记录与设定其 IP 地址，当计算机开机后，就可从路由器自动取得 IP 地址，管理方便。

起始 IP 地址： 系统默认为四个网段从 192.168.1.100、192.168.2.100、192.168.3.100、192.168.4.100 的 IP 地址开始发放。您可以依照实际需求来设定。

终止 IP 地址： 系统默认为四个网段 192.168.1.149、192.168.2.149、192.168.3.149、192.168.4.149IP 地址为最后发放 IP，也就是说出厂设定值每个网段可供 50 台计算机自动取得 IP 地址 四个网段共 200 台计算机自动取得 IP 地址。您可以依照实际需求来设定。

6.1.3 广域网络 WAN 及非军事区设置

广域网网络连接型态设置：

广域网线路配置

接口位置	连接类型	配置
广域网1	自动取得 IP 地址	编辑
广域网2	指定 IP 地址	编辑

接口位置：广域网连线所在 WAN 接口位置。

线路连接类型状态：此项显示该广域网口目前设置的联机状态。安全路由器提供五种联机状态设置：自动取得 IP 地址；固定 IP 地址；PPPoE 拨号联机；PPTP 拨号联机以及透明桥接模式。

配置：点击“编辑”按钮可以进入广域网联机状态的设置窗口。各类型的联机状态设置请参考以下的说明，并选择配合运营商所给您的联机状态来做设置。

自动取得 IP 地址（动态获得 IP 地址/DHCP 用户）：

此为安全路由器系统默认的联机方式，此联机方式为 DHCP 客户端自动取得 IP 模式，多为应用于如线缆调制解调器或是 DHCP 客户端联机状态等连接，若您的联机为其它不同的方式，请选取相关的设置并参考以下的介绍做设置。

在自动取得 IP 模式，您可以使用自定 DNS 的 IP 地址，勾选此选项并填入您要使用的 DNS 服务器 IP 地址。

接口位置: WAN1

广域网连接类型: 动态获得 IP 地址(DHCP用户)

☑ 使用以下的DNS服务器IP地址

DNS 服务器(首选): 0 . 0 . 0 . 0

DNS 服务器(备用): 0 . 0 . 0 . 0

☑ 激活掉线排程

广域网掉线时间: 从 : 到 : (时间格式:24小时制)

掉线排程: 分钟前开始转移新的会话

指定备援接口: 关闭

共享式广域网环境: ○ 是 ⦿ 否 (防止收到来自其他广域网的广播封包)

MTU: ⦿ 自动 ○ 手动 1500 bytes

返回 确定 取消

使用以下的 DNS 服务器 IP 地址：	选择使用自定的 DNS 服务器 IP 地址。
DNS 服务器：	输入您的运营商所提供的动态域名解析服务器 IP 地址，最少填入一组，最多可填二组。
广域网掉线排程：	勾选此项目会启用广域网掉线排程的机制。在某些区域，广域网的联机服务会有时间的限制，例如从凌晨 12:00 到清晨 6:00 之间六个小时，光纤联机服务会中断。虽然安全路由器有备援机制，此操作当此广域网断线的瞬间，所有经由该广域网对外访问的联机也会因此中断，重新连接时，才会经由备援机制走其它广域网出去。因此，为了避免在广域网断线的瞬间大量的联机被切断，您可以启用此机制在此广域网断线前一段时间，先将新增的联机经由其它广域网出去外网访问，可以减少此广域网断线时的冲击。
广域网掉线时间：	输入此广域网中断连接服务的规则时间。

掉线排程： 输入您希望在此广域网中断连接服务之前多长时间开始将新增的联机经由其它广域网出去外网访问。

指定备援接口： 若是此广域网有设置端口绑定，请选择要由哪一个广域网口做备援。通常您应该选择与此广域网同一个运营商联机的广域网口。

共享式广域网环境： 若您的广域网线路有连接至交换机(Switch)，可以点选「是」将此功能开启，来屏避掉不需要的广播数据包，增加您网络使用的效能与安全性，默认值「否」则是将此功能关闭。

MTU: MTU 为 Maximum Transmission Unit 的缩写，可选自动或手动来控制，一般默认为 1500。 但是在不同的网络环境中，可能会使用不同的数值。尤以 ADSL PPPoE 的状况为最多(ADSL PPPoE MTU 值：1492)。一般使用默认 Auto 即可，不需做任何调整。

点击此按钮"确认"即会存储刚才所变动的修改设置内容参数，点击此按钮"取消"即会清除刚才所变动的修改设置内容参数，此操作必须于确认存储动作之前才会有效。

固定 IP 地址联机（指定 IP 地址）：

若您的运营商有核发固定的 IP 地址给您(如 1 个 IP 或是 8 个 IP 等)，请您选择此种方式联机，将运营商所核发的 IP 信息分别参照以下介绍填入相关设置参数中。

接口位置: WAN1

广域网连接类型： 指定IP 位址(固定IP或ADSL专线用户)

广域网 IP地址： 0 . 0 . 0 . 0

子网掩码： 0 . 0 . 0 . 0

默认网关： 0 . 0 . 0 . 0

DNS 服务器(首选)： 0 . 0 . 0 . 0

DNS 服务器(备用)： 0 . 0 . 0 . 0

☑ **激活掉线排程**

广域网掉线时间： 从 : 到 : (时间格式:24小时制)

掉线排程： 分钟前开始转移新的会话

指定备援接口： 关闭

共享式广域网环境： ○ 是 ◉ 否 (防止收到来自其他广域网的广播封包)

MTU： ◉ 自动 ○ 手动 1500 bytes

返回 确定 取消

广域网 IP 地址： 输入您的运营商所核发的可使用固定 IP 地址的其中一个。

子网掩码： 输入您的运营商所核发的可使用固定 IP 地址的子网掩码，如：
发放 8 个固定 IP 地址：255.255.255.248
发放 16 个固定 IP 地址：255.255.255.240

默认网关： 输入您的运营商所核发的可使用固定 IP 地址的默认网关，若您是使用 ADSL 的话，一般说来都是 ADSL 数据机（ATU-R）的 IP 地址。

DNS 服务器： 输入您的运营商所规定的名称解析服务器 IP 地址，最少填入一组，最多可填二组。

广域网掉线排程： 勾选此项目会启用广域网掉线排程的机制。在某些区域，广域网的联机服务会有时间的限制，例如从凌晨 12:00 到清晨 6:00 之间六个小时，光纤联机服务会中断。虽然安全路由器有备援机制，此操作当此广域网断线的瞬间，所有经由该广域网对外访问的联机也会因此中断，重新连接时，才会经由备援机制走其它广域网出去。因此，为了避免在广域网断线的瞬间大量的联机被切断，您可以启用此机制在此广域网断线前一段时间，先将新增的联机经由其它广域网出去外网访问，可以减少此广域网断线时的冲击。

广域网掉线时间： 输入此广域网中断连接服务的规则时间。

掉线排程： 输入您希望在此广域网中断连接服务之前多长时间开始将新增的联机经由其它广域网出去外网访问。

指定备援接口： 若是此广域网有设置端口绑定，请选择要由哪一个广域网口做备援。通常您应该选择与此广域网同一个运营商联机的广域网口。

共享式广域网环境： 若您的广域网线路有连接至交换机(Switch)，可以点选「是」将此功能开启，来屏避掉不需要的广播数据包，增加您网络使用的效能与安全性，默认值「否」则是将此功能关闭。

MTU: MTU 为 Maximum Transmission Unit 的缩写，可选自动或手动来控制，一般默认为 1500。 但是在不同的网络环境中，可能会使用不同的数值。尤以 ADSL PPPoE 的状况为最多(ADSL PPPoE MTU 值：1492)。一般使用默认 Auto 即可，不需做任何调整。

点击此按钮“确认”即会存储刚才所变动的修改设置内容参数，点击此按钮“取消”即会清除刚才所变动的修改设置内容参数，此操作必须于确认存储动作之前才会有效。

PPPoE 拨号联机：

此项为 ADSL 虚拟拨号使用(适用于 ADSL PPPoE)，填入运营商给予的使用者联机名称与密码并以安全路由器内建的 PPP Over Ethernet 软件联机，若是您的 PC 之前已经有安装由运营商所给予的 PPPoE 拨号软件的话，请将其移除，不需要再使用此个别连接网络。

接口位置: WAN1

广域网连接类型： PPPoE 设定(ADSL拨接用户)

用户名：

密码：

闲置 5 分钟自动断线.

保持连接，如断线 30 秒后自动重新连接

激活掉线排程

广域网掉线时间： 从 : 到 : (时间格式:24小时制)

掉线排程： 分钟前开始转移新的会话

指定备援接口： 关闭

共享式广域网环境： 是 否 (防止收到来自其他广域网的广播封包)

MTU： 自动 手动 1500 bytes

返回 确定 取消

用户名：	输入您的运营商所核发的使用者名称。
密码：	输入您的运营商所核发的使用密码。
闲置( )分钟自动断线：	此功能能够让您的 PPPoE 拨接连线能够使用自动拨号功能，当使用端若是有上网需求时，安全路由器 会自动向默认的运营商自动拨号联机，当网络一段时间闲置无使用时，则系统会自动离线。您可以自行输入所需要的无数据包传送自动离线等待时间，默认为 5 分钟。
保持连接：	此功能能够让您的 PPPoE 拨接连线能够断线自动重拨，您可以自行设置重新拨接的时间，默认值为 30 秒。

广域网掉线排程：　勾选此项目会启用广域网掉线排程的机制。在某些区域，广域网的联机服务会有时间的限制，例如从凌晨 12:00 到清晨 6:00 之间六个小时，光纤联机服务会中断。虽然安全路由器有备援机制，但是当此广域网断线的瞬间，所有经由该广域网对外访问的联机也会因此中断，重新连接时，才会经由备援机制走其它广域网出去。因此，为了避免在广域网断线的瞬间大量的联机被切断，您可以启用此机制在此广域网断线前一段时间，先将新增的联机经由其它广域网出去外网访问，可以减少此广域网断线时的冲击。

广域网掉线时间：　输入此广域网中断连接服务的规则时间。

掉线排程：　输入您希望在此广域网中断连接服务之前多长时间开始将新增的联机经由其它广域网出去外网访问。

指定备援接口：　若是此广域网有设置端口绑定，请选择要由哪一个广域网口做备援。通常您应该选择与此广域网同一个运营商联机的广域网口。

共享式广域网环境：　若您的广域网线路有连接至交换机(Switch)，可以点选「是」将此功能开启，来屏避掉不需要的广播数据包，增加您网络使用的效能与安全性，默认值「否」则是将此功能关闭。

MTU:　MTU 为 Maximum Transmission Unit 的缩写，可选自动或手动来控制，一般默认为 1500。 但是在不同的网络环境中，可能会使用不同的数值。尤以 ADSL PPPoE 的状况为最多(ADSL PPPoE MTU 值：1492)。一般使用默认 Auto 即可，不需做任何调整。

点击此按钮“确认”即会存储刚才所变动的修改设置内容参数，点击此按钮“取消”即会清除刚才所变动的修改设置内容参数，此操作必须于确认存储动作之前才会有效。

PPTP 拨号联机：

此项为 PPTP (Point to Point Tunneling Protocol) 计时制使用，填入运营商给予的使用者联机名称与密码并以安全路由器内建的 PPTP 软件联机。

接口位置: WAN1

广域网连接类型: PPTP 设定(ADSL拨接PPTP用户)

广域网 IP地址: 0 . 0 . 0 . 0

子网掩码: 0 . 0 . 0 . 0

默认网关: 0 . 0 . 0 . 0

用户名:

密码:

○ 闲置 5 分钟自动断线.

⊙ 保持连接，如断线 30 秒后自动重新连接

☑ 激活掉线排程

广域网掉线时间: 从 : 到 : (时间格式:24小时制)

掉线排程: 分钟前开始转移新的会话

指定备援接口: 关闭

共享式广域网环境: ○ 是 ⊙ 否 (防止收到来自其他广域网的广播封包)

MTU: ⊙ 自动 ○ 手动 1500 bytes

返回 确定 取消

广域网 IP 地址：	输入您的运营商所核发的可使用固定 IP 地址的其中一个。
子网掩码：	输入您的运营商所核发的可使用固定 IP 地址的子网掩码。
默认网关：	输入您的运营商所核发的可使用固定 IP 地址的默认网关，若您是使用 ADSL 的话，一般说来都是 ATU-R 的 IP 地址。
用户名：	输入您的运营商所核发的使用者名称。
密码：	输入您的运营商所核发的使用密码。
闲置( )分钟自动断线：	此功能能够让您的 PPTP 拨接连线能够使用自动拨号功能，当使用端若是有上网需求时，安全路由器 会自动向默认的运营商自动拨号联机，当网络一段时间闲置无使用时，则系统会自动离线。无数据包传送的自动离线时间默认为 5 分钟，您可以自行输入所需要的自动离线等待时间。

保持连接：	此功能能够让您的 PPTP 拨接连线能够断线自动重拨，而且可以自行设置重新拨接的时间，默认值为 30 秒。
广域网掉线排程：	勾选此项目会启用广域网掉线排程的机制。在某些区域，广域网的联机服务会有时间的限制，例如从凌晨 12:00 到清晨 6:00 之间六个小时，光纤联机服务会中断。虽然安全路由器有备援机制，但是当此广域网断线的瞬间，所有经由该广域网对外访问的联机也会因此中断，重新连接时，才会经由备援机制走其它广域网出去。因此，为了避免在广域网断线的瞬间大量的联机被切断，您可以启用此机制在此广域网断线前一段时间，先将新增的联机经由其它广域网出去外网访问，可以减少此广域网断线时的冲击。
广域网掉线时间：	输入此广域网中断连接服务的规则时间。
掉线排程：	输入您希望在此广域网中断连接服务之前多长时间开始将新增的联机经由其它广域网出去外网访问。
指定备援接口：	若是此广域网有设置端口绑定，请选择要由哪一个广域网口做备援。通常您应该选择与此广域网同一个运营商联机的广域网口。
共享式广域网环境：	若您的广域网线路有连接至交换机(Switch)，可以点选「是」将此功能开启，来屏避掉不需要的广播数据包，增加您网络使用的效能与安全性，默认值「否」则是将此功能关闭。
MTU:	MTU 为 Maximum Transmission Unit 的缩写，可选自动或手动来控制，一般默认为 1500。 但是在不同的网络环境中，可能会使用不同的数值。尤以 ADSL PPPoE 的状况为最多(ADSL PPPoE MTU 值：1492)。一般使用默认 Auto 即可，不需做任何调整。

点击此按钮“确认”即会存储刚才所变动的修改设置内容参数，点击此按钮“取消”即会清除刚才所变动的修改设置内容参数，此操作必须于确认存储动作之前才会有效。

透通桥接模式（Transparent Bridge）：

当您内网的计算机 IP 已经都是公网 IP 而不希望将内网都改成私网 IP(例如 192.168.1.X)时，此功能可以让您不需更动原有架构，立即整合到既有网络中。选择广域网联机方式为透明桥接模式，这样您可以保留内网计算机的 IP 设置为原本的公网 IP 仍然可以正常上网。

当您设置两个广域网时，广域网的联机模式选择此种透明桥接模式，还是可以做到负载均衡。

接口位置: WAN1
广域网连接类型: Transparent Bridge (透通桥接模式)
广域网 IP地址: 0 . 0 . 0 . 0
子网掩码: 0 . 0 . 0 . 0
默认网关: 0 . 0 . 0 . 0
DNS 服务器(首选): 0 . 0 . 0 . 0
DNS 服务器(备用): 0 . 0 . 0 . 0
公网IP地址范围 1: 0 . 0 . 0 . 0 到 0
公网IP地址范围 2: 0 . 0 . 0 . 0 到 0
☑ 激活掉线排程
广域网掉线时间: 从 : 到 : (时间格式:24小时制)
掉线排程: 分钟前开始转移新的会话
指定备援接口: 关闭
共享式广域网环境: ○ 是 ◉ 否 (防止收到来自其他广域网的广播封包)
MTU: ◉ 自动 ○ 手动 1500 bytes
返回 确定 取消

广域网 IP 地址： 输入您的运营商所核发的可使用固定 IP 地址的其中一个。

子网掩码： 输入您的运营商所核发的可使用固定 IP 地址的子网掩码，如：255.255.255.240

默认网关： 输入您的运营商所核发的可使用固定 IP 地址的默认网关，若您是使用 ADSL 的话，一般说来都是 ATU-R 的 IP 地址。

DNS 服务器： 输入您的运营商所规定的名称解析服务器 IP 地址，最少填入一组，最多可填二组。

公网 IP 地址范围： 输入您的运营商所核发的可使用固定 IP 范围。若是您的运营商分给您两个不连续的 IP 地址范围，您可以分别填入。

广域网掉线排程：	勾选此项目会启用广域网掉线排程的机制。在某些区域，广域网的联机服务会有时间的限制，例如从凌晨 12:00 到清晨 6:00 之间六个小时，光纤联机服务会中断。虽然安全路由器有备援机制，但是当此广域网断线的瞬间，所有经由该广域网对外访问的联机也会因此中断，重新连接时，才会经由备援机制走其它广域网出去。因此，为了避免在广域网断线的瞬间大量的联机被切断，您可以启用此机制在此广域网断线前一段时间，先将新增的联机经由其它广域网出去外网访问，可以减少此广域网断线时的冲击。
广域网掉线时间：	输入此广域网中断连接服务的规则时间。
掉线排程：	输入您希望在此广域网中断连接服务之前多长时间开始将新增的联机经由其它广域网出去外网访问。
指定备援接口：	若是此广域网有设置端口绑定，请选择要由哪一个广域网口做备援。通常您应该选择与此广域网同一个运营商联机的广域网口。
共享式广域网环境：	若您的广域网线路有连接至交换机(Switch)，可以点选「是」将此功能开启，来屏避掉不需要的广播数据包，增加您网络使用的效能与安全性，默认值「否」则是将此功能关闭。
MTU:	MTU 为 Maximum Transmission Unit 的缩写，可选自动或手动来控制，一般默认为 1500。 但是在不同的网络环境中，可能会使用不同的数值。尤以 ADSL PPPoE 的状况为最多(ADSL PPPoE MTU 值：1492)。一般使用默认 Auto 即可，不需做任何调整。

点击此按钮“确认”即会存储刚才所变动的修改设置内容参数，点击此按钮“取消”即会清除刚才所变动的修改设置内容参数，此操作必须于确认存储动作之前才会有效。

路由 NAT 混合模式

当您申请的线路连线方式是使用公网 IP 而且必须使用路由模式来与局端连线，此功能可以让您内网计算机的 IP 设定为这条线路所需要使用的公网 IP 来正常上网，其余设为私有 IP 的计算机一样可以经由 NAT 方式来正常上网。

当您设定多个广域网时，广域网的连线模式选择此种路由 NAT 混合模式，还可以做到负载均衡。

接口位置: WAN1

字段	值
广域网 线路连线类型：	路由NAT混合模式
广域网 IP地址：	0 . 0 . 0 . 0
子网掩码：	255 . 255 . 255 . 0
预设网关：	0 . 0 . 0 . 0
DNS服务器(主要)：	0 . 0 . 0 . 0
DNS服务器(次要)：	0 . 0 . 0 . 0
路由网关 1:	0 . 0 . 0 . 0
公网IP地址范围 1:	0 . 0 . 0 . 0 到 0
公网IP地址范围 2:	0 . 0 . 0 . 0 到 0
路由网关 2:	0 . 0 . 0 . 0
公网IP地址范围 1:	0 . 0 . 0 . 0 到 0
公网IP地址范围 2:	0 . 0 . 0 . 0 到 0
路由网关 3:	0 . 0 . 0 . 0
公网IP地址范围 1:	0 . 0 . 0 . 0 到 0
公网IP地址范围 2:	0 . 0 . 0 . 0 到 0

广域网络 IP 地址： 输入您的运营商所提供与局端连线的路由 IP 地址。

子网掩码： 输入您的运营商所提供与局端连线的路由 IP 地址的子网掩码，如：255.255.255.240

广域网默认网关： 输入您的运营商所所提供与局端连线的路由 IP 地址的默认网关。

DNS 服务器： 输入您的运营商所规定的名称解析服务器 IP 地址，最少填入一组，最多可填二组。

路由网关： 输入您的运营商所核发的可使用固定 IP 范围的其中一个 IP 地址作为预设网关。

公网 IP 地址范围： 输入您的运营商所核发的可使用固定 IP 范围。若是您的运营商分给您两个不连续的 IP 地址范围，您可以分别填入“局域网 IP 地址范围 1”以及“局域网 IP 地址范围 2”。
若是您的运营商分给您多个不同子网段的 IP 地址范围，您可以填入其它的”局域网络由预设网关”以及” 局域网 IP 地址范围”。

非军事区(DMZ)：

对于某些网络环境应用来说，可能会需要用到独立的 DMZ 非军事管制区接口来置放对外服务服务器，如 WWW 网页服务器与 Mail 电子邮件服务器等等。侠诺的安全路由器提供您独立的 DMZ 接口来设定连接有合法 IP 地址的服务器。此 DMZ 接口是从网络或局域网存取对外服务器内容的沟通桥梁。

☑ **激活此选项会设定 DMZ 端口**

DMZ 配置

端口	线路连线类型	配置
DMZ	0.0.0.0	编辑

确定 取消

IP 地址：此项显示您给予 DMZ 端口的 IP 地址或范围。

配置：点击“编辑”按钮可以进入 DMZ 的设置窗口。请参考以下的设定说明。

此 DMZ 的设定可分为 **Subnet**、**Range**、以及 **与路由 NAT 混合模式局域网 IP 同网段** 三种：

Subnet：

DMZ 与广域网络 WAN 要在不同的子网络 Subnet 中。

就是若运营商端分配给您 16 个合法 IP 如：220.243.230.1-16/子网掩码：255.255.255.240 时，您必须将此 16 个 IP 再切两组变成 220.243.230.1-8 /子网掩码：255.255.255.248 及另一组 220.243.230.9-16/子网掩码：255.255.255.248，然后路由器及网关是在同一组，再将另一组设定在 DMZ 中。

接口位置 ：DMZ

Subnet　Range (DMZ与广域网口IP地址相同子网掩码)　DMZ与路由及NAT混合模式局域网IP同网段

DMZ IP地址: 0 . 0 . 0 . 0
子网掩码: 255 . 255 . 255 . 0

共享式广域网环境: 激活　关闭 (防止收到来自其他广域网的广播封包)

返回　確定　取消

DMZ IP 地址：　输入在 DMZ 端口的 IP 代表地址。

子网掩码：　输入在 DMZ 端口的 IP 子网掩码。

Range：

DMZ 与广域网络 WAN 位在相同的子网络 Subnet。

接口位置 ：DMZ

Subnet　Range (DMZ与广域网口IP地址相同子网掩码)　DMZ与路由及NAT混合模式局域网IP同网段

接口位置 ：
IP地址范围: 0 . 0 . 0 . 0 to 255

共享式广域网环境: 激活　关闭 (防止收到来自其他广域网的广播封包)

返回　確定　取消

接口位置：　选择 DMZ 是与哪一个 WAN 口的 IP 地址在相同的子网掩码。

IP 地址范围：　输入在 DMZ 端口的 IP 范围。

DMZ 与路由 NAT 混合模式局域网 IP 同网段：

DMZ 与路由 NAT 混合模式的局域网 IP 地址在相同的子网段。

接口位置：DMZ

○ Subnet ○ Range (DMZ与广域网口IP地址相同子网掩码) ⊙ DMZ与路由及NAT混合模式局域网IP同网段

接口位置：

路由网关1: 0 . 0 . 0 . 0

公网IP地址范围 0 . 0 . 0 . 0 to 0

路由网关2: 0 . 0 . 0 . 0

公网IP地址范围 0 . 0 . 0 . 0 to 0

路由网关3: 0 . 0 . 0 . 0

公网IP地址范围 0 . 0 . 0 . 0 to 0

共享式广域网环境: ○ 激活 ⊙ 关闭 (防止收到来自其他广域网的广播封包)

返回 確定 取消

局域网络由预设网关： 输入您在"路由 NAT 混合模式"所设定的局域网路由预设网关。

局域网 IP 地址范围： 输入您的运营商所核发的可使用固定 IP 范围中您要用来作为 DMZ 服务器的 IP 范围。

若是您的运营商分给您多个不同子网段的 IP 地址范围，您可以填入其它的"局域网络由预设网关"以及" 局域网 IP 地址范围"。

点击此按钮"**确认**"即会存储刚才所变动的修改设定内容参数，点击此按钮"**取消**"即会清除刚才所变动的修改设定内容参数，此操作必须于确认存储动作之前才会有效。

6.2 多 WAN 设置

当用户的连线是采用多 WAN 的线路设计，管理人员可以进入网络连线设置的流量管理、与协议绑定栏目，对安全路由器的负载均衡模式等进行设置，使安全路由器达到最优数据转发是网络带宽效能达到最高。

模式

智能型负载均衡	均衡模式:	◉ 连机数均衡 高级设置	○ IP 均衡
指定路由	未绑定端口均衡模式:	○ 连机数均衡 高级设置	○ IP 均衡
策略路由	均衡模式:	○ 连机数均衡 高级设置	○ IP 均衡
	广域网组合设定		
	联通策略 关闭	更新网段	
	自定义策略1 关闭		
	自定义策略2 关闭		

端口

端口	模式	配置
广域网1	全自动	编辑
广域网2	全自动	编辑

线路侦测机制

	端口	广域网1
☑	激活	
	重新发起测试次数	5
	响应延迟时间	30 秒
	当线路连接失败时	移除该条线路
☑	当上传 或 下载流量超过 1 %, 不进行线路侦测.	
☑	预设网关 IP 地址	
☑	ISP 服务器	168.95.1.1
☑	远程服务器	168.95.192.1
☐	使用 DNS 服务器作域名解析	

6.2.1 负载均衡模式

模式

智能型负载均衡	均衡模式:	连机数均衡 高级设置	IP 均衡
指定路由	未绑定端口均衡模式:	连机数均衡 高级设置	IP 均衡
策略路由	均衡模式:	连机数均衡 高级设置	IP 均衡
	广域网组合设定		
	联通策略 关闭 更新网段		
	自定义策略1 关闭		
	自定义策略2 关闭		

智能型负载均衡模式：

当您选用智能负载均衡模式，安全路由器将以会话数或是 IP 地址会话数为基础，并依据您广域网线路的带宽来自动分配会话，达到对外会话的负载均衡。线路的带宽是依据您所填入的带宽设置(请参考下一小节设置说明)，例如当两条广域网都为上行 512Kbit/sec 时，其自动负载比例为 1:1，当一条线路的上行带宽为 1024kbit/sec 另一条为 512kbit/sec 时，则此自动负载比例为 2:1，所以为了确保您的安全路由器达到实际线路负载能够均衡，请填入实际上行下载带宽（请参考下一段 QoS 节带宽管理设置说明)。

依会话数均衡：当您选用会话数均衡模式，安全路由器将以会话数为基础，并依据您广域网线路的带宽来自动分配会话，达到会话的负载均衡。

依 IP 地址均衡：当您选用 IP 负载均衡模式，安全路由器将以会话的 IP 数为基础，并依据您广域网线路的带宽来自动分配会话，达到会话的负载均衡。

提示！

不论是会话数均衡或是 IP 负载均衡方式，搭配"通讯协议绑定"可以有更弹性运用您的带宽，您可将特定的内网 IP，使用特定应用服务端口作访问，或特定的目的地 IP 经由您指定的广域网来访问外网。

譬如您希望指定 IP 192.168.1.100 访问外网的时候走广域网 1，或内网所有 IP 去访问服务端口 80 时都是经过广域网 2，或是内网所有 IP 去目的地 IP 211.1.1.1 访问时要从广域网 1 去访问等等，都可以经由设置此"通讯协议绑定"功能来达到您的需求。请注意，当使用智能负载均衡方式搭配"通讯协议绑定"功能时，除了您指定的访问会按照您的规则出去访问外网，其它未被指定的 IP 或服务端口的访问还是按照安全路由器的机制做智能负载均衡。

关于如何设置"通讯协议绑定"功能，以及智能负载均衡方式搭配"通讯协议绑定"的范例，请参考 （6.2.3 节的通讯协议绑定设置说明）。

指定路由：

这个模式让您对特定的内网 IP、特定要访问的应用服务端口、或特定目的地 IP 经由您指定的广域网对外网做访问。且一经指定后，该广域网也只能让这些指定的内网 IP、特定要访问的应用服务端口、或特定目的地 IP 使用。

其它不在这些指定的内网 IP、特定要访问的应用服务端口、或特定目的地 IP 都会从其它的广域网出去访问。对于没有被指定的广域网，您可以选择他们的负载均衡模式是以会话数作为负载均衡的基础，还是以 IP 会话数作为负载均衡的基础。

未绑定端口均衡模式：若是有部分广网端口并没有被指定，以 2WAN 的路由器产品为例，若广域网 2 没有指定特定的 IP、服务端口、或目的 IP 来使用，则广域网 2 仍然会依据安全路由器的负载均衡机制来分配会话。均衡机制如下：

依会话数均衡：当您选用会话数均衡模式，安全路由器将以会话数为基础，并依据您广域网线路的带宽来自动分配会话，达到会话的负载均衡。

依 IP 地址均衡：当您选用 IP 负载均衡模式，安全路由器将以会话的 IP 数为基础，并依据您广域网线路的带宽来自动分配会话，达到会话的负载均衡。

提示！

此指定路由必须配合"通讯协议绑定"功能才能发挥作用。例如指定让内网去访问服务端口 80 时都要从广域网 1 去访问，或内网去目的地 IP 211.1.1.1 访问时要从广域网 1 去访问等等，必须要在"通讯协议绑定"功能中做设置。要注意，当使用指定路由(Exculsive Mode)模式，以上述的例子来看，除了您指定的访问必须按照您的规则出去访问外网都走广域网 1 以外，其它未被指定的 IP 或服务端口则经由安全路由器负载均衡的机制使用其它的广域网出去。

关于如何设置"通讯协议绑定"功能，以及指定路由模式搭配"通讯协议绑定"的范例，请参考（6.2.3 节的通讯协议绑定设置说明）。

策略路由：

当您选用策略路由模式，安全路由器会依照内建的策略(电信、网通)自动分配会话。您只需选择网通线路接入的广域网口(或广域网组合)，安全路由器会自动将该走网通线路去外网访问的流量都从网通的广域网出去；对该走电信线路去外网访问的流量也都会往电信的广域网出去，达到"电信走电信，网通走网通"的分流策略。

广域网组合设置：

当您所接的网通线路不只一条，则需要做广域网的组合，以便将两个以上的广域网口合在一起做相同的策略分流。点击"广域网组合设置"会弹出以下的对话窗口。

*此为示意图，会因产品线不同，图形会有所差异

名称：	在此自定的广域网组合名称，如"教育"等，用来辨识广域网群组。
接口位置：	在此勾选要设在此组合的广域网口。
增加到对应列表：	增加到广域网组合列表。
删除选中的项目：	删除所选择的广域网组合内容。
确定：	点击此按钮"确认"即会存储刚才所变动的修改设置内容参数。
取消：	点击此按钮"取消"即会清除刚才所变动的修改设置内容参数，此操作必须于确认存储动作之前才会有效。
关闭：	关闭并离开此功能设置窗口。

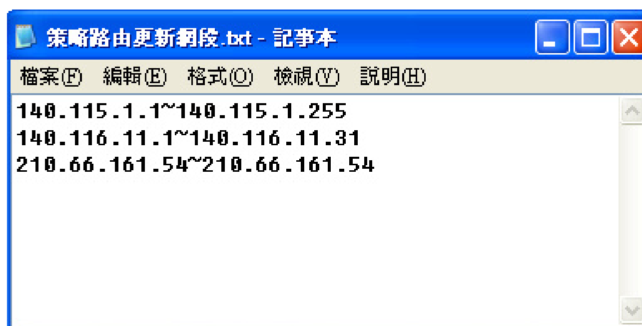
设置完成后，您就可以在网通策略的选择中选取您的网通接口的广域网组合。

自定策略：

此外，您也可以自己建立分流策略。在"自定策略"中选择要指定的广域网口或广域网组合(例如广域网 1)，然后点击"更新策略"的按键，会出现汇入策略文件的对话窗口。策略文件是一个可编辑的文本文件，应含有您指定的目的 IP 地址。将文件汇入路径选择好之后，点击"汇入"，并在设置窗口的最下方点击"确定"，安全路由器就

会将要往指定目的 IP 的流量从您指定的广域网(例如广域网 1)或广域网组合出去。

策略文件的建立可以用纯文本编辑软件来撰写，例如使用 Windows 系统自带的文本编辑程序"记事本"来建立。将您要指定的目的 IP 地址按照下图的格式写入，例如您要指定的目的 IP 地址范围是从 140.115.1.1 到 140.115.1.255，则在"记事本"中输入 140.115.1.1～140.115.1.255。下一个目的 IP 地址范围则要换行输入。请注意！若是只有一个目的 IP 地址，也需要以同样的格式来书写。例如指定的目的 IP 地址是 210.66.161.54，则必须写成 210.66.161.54～210.66.161.54 格式。存储文件后(扩展名应该是.txt)即可汇入自定策略的更新网段。



提示！

网通策略与自定策略可以同时存在，但当某一个目的 IP 同时在网通策略以及自定策略中，则会以网通策略优先执行。也就是说要往该目的 IP 的流量会从网通策略的广域网(或广域网组合)出去外网。

连机数(会话数)均衡高级设定

一般会话数均衡是平均与随机分配每个内网 IP 的会话数量，但是某些较特殊的连线例如网络银行的加密连线(Https、TCP443) 需要固定从同一个 WAN IP 建立才能够正常操作，所以当同一个内网 IP 访问网络银行网站，访问操作动作被会话数均衡机制分配到不同 WAN IP 去建立连线时，有可能就会在操作过程中发生断线或不正常的状况，而连线均衡的高级设定功能就是用来解决这个问题。

高级设定可以设定同一个内网 IP，在以某个特殊的服务通讯端口建立连线时，固定从某一个 WAN IP 去建立，其它类型的服务通讯端口连线仍然照原来的均衡机制随机平均分配，除了可达成原来会话数均衡所带来的效用

之外，也可确定一些较特殊的服务通讯端口连线时能正常运作。

模式

智能型负载均衡	均衡模式:	◉ 连机数均衡 高级设置	○ IP 均衡
指定路由	未绑定端口均衡模式:	○ 连机数均衡 高级设置	○ IP 均衡
策略路由	均衡模式:	○ 连机数均衡 高级设置	○ IP 均衡
	广域网组合设定		
	联通策略 关闭 更新网段		
	自定义策略1 关闭		
	自定义策略2 关闭		

点选 高级设置 进入设定选单：

◉ 目的地会话登录自动绑定
○ 用户自定义目的地及服务端口绑定

无闲置机制

通讯协定 两者
服务端口范围 ______ 到 ______
增加到对应列表

TCP[1863~1863]
TCP[5050~5050]
UDP[8000~8005]

删除所选择对应项目

确定 取消 退出

目的地会话登录自动绑定： 选择此选项表示到目的地 IP 地址位于同一个 Class B 范围子网时，就固定从同一个 WAN IP 建立连线。

举例来说，总共两个 WAN1 200.10.10.1 与 WAN2 200.10.10.2，内网两个 IP 192.168.1.100 与 192.168.1.101，192.168.1.100 首次去访问外网 61.222.81.100 时，被随机分配到以 WAN1 200.10.10.1 建立连线，当 192.168.1.100 有下一笔连线目的地是 61.222.81.101 (在同一个 Class B 子网范围) 时，也一样会以 WAN1 200.10.10.1 去建立连线，但是若是去到别的目的地 IP (不在 61.222.81.100 同一个 Class B 子网范围) 则依然以原来会话数均衡的机制随机平均分配。

另一个内网 IP 192.168.1.101，首次去访问外网 61.222.81.101 时，被随机分配到以 WAN2 200.10.10.2 建立连线，当 192.168.1.101 有下一笔连线目的地是 61.222.81.100 (在同一个 Class B 子网范围) 时，也一样会以 WAN2 200.10.10.2 去建立连线，但是若是去到别的目的地 IP (不在 61.222.81.100 同一个 Class B 子网范围) 则依然以原来会话数均衡的机制随机平均分配。

※请注意！
并不是「所有内网 IP」到某一「相同 Class B 范围」都固定以某个 WAN IP 进行连线，而是看「每一个内网 IP」第一次被随机分配到以那一个 WAN IP 进行连线，之后遇到目的地是相同 Class B 范围，再「个别」按照同一个 WAN IP 进行连线。

无闲置机制：

单一 IP 所设定的服务端口，在会话数负载均衡预设功能下，不会因为闲置一段时间没流量，被系统断线清除。

通讯协议：选择 TCP 或 UDP 或 TCP 与 UDP 两者。

服务端口范围：设定无闲置机制的服务端口范围，如果上方的通讯协议是选择「两者」，则是同时指 TCP 与 UDP 的服务端口范围，例如两者 [123~125]」就是表示 TCP 123~125 端口「与」UDP 123~125 端口。

用户自定义目的地及服务端口绑定：

这边是设定单一内网 IP，以某个自定义的特殊服务通讯向某个目的地 IP (或 IP 范围) 进行连线时，固定以同一个 WAN IP 进行连线。

您可以自行设定服务通讯端口与目的地 IP 内容 (目的地 IP 范围若设定成 0.0.0.0 到 0 表示到「任何一个目的地 IP 范围」

※请注意！
「用户自定义目的地及服务端口绑定」与「目的地连线登入自动绑定」两者只能同时使用其中一种！

以出厂预设已有设定的规则举例： (如下图)

○ 目的地会话登录自动绑定
◉ 用户自定义目的地及服务端口绑定

服务端口： All Traffic [TCP&UDP/1~65535]

服务端新增或删除表

目的 IP 地址 [ ] . [ ] . [ ] . [ ]

激活： ☐

增加到对应列表

HTTPS [TCP/443~443]->0.0.0.0~0.0.0.0

删除所选择对应项目

确定 取消 退出

表示内网任何单一 IP，在以 TCP 443 Port 与任何目的地 (0.0.0.0 到 0 表示任何目的地) 进行连线时，都固定以同一个 WAN IP 进行连线，至于各个内网 IP 的选择是固定在那一个 WAN IP，则是以第一次被原本会话数均衡机制所随机分配到的 WAN IP 为准，举例来说两个内网 IP 192.168.100.1 与 192.168.100.2，当个别第一次进行 TCP 443 Port 连线时，192.168.100.1 被随机平均分配到以 WAN 1 IP 连线，192.168,100.2 被随机分配到以 WAN2 IP 连线，则只要之后 192.168.100.1 有任何 TCP 443 Port 的连线，就会固定以 WAN 1 IP 连线；192.168.100.2 有任何 TCP 443 Port 的连线，就会固定以 WAN 2 IP 连线。

此预设规则虽然出厂默认值就有，但是您可以视自己的需求取消/删除此规则的应用，或新增其它新的规则以符合实际的连线需求。

6.2.2 线路侦测机制

若勾选此项设置，则会显示出重新发起测试次数，响应延长时间等信息。当使用两条广域网做对外联结线路时一定将此 NSD 启用，以避免因为广域端口流量过大时造成 QoS 安全路由器的误判将此线路判断为断线。

线路侦测机制

	端口	广域网1
☑	激活	
	重新发起测试次数	5
	响应延迟时间	30 秒
	当线路连接失败时	移除该条线路
☑	当上传 或 下载流量超过 1 %, 不进行线路侦测.	
☑	预设网关 IP 地址	
☑	ISP 服务器	168.95.1.1
☑	远程服务器	168.95.192.1
☐	使用 DNS 服务器作域名解析	

接口位置： 选择您要设置线路侦测的广域网口。

重新发起测试次数： 对外会话侦测重试次数，默认值为五次。如果会话侦测重试次数超过设置次数，网络没有回应的话，则判断为对外线路中断！

响应延迟时间： 对外会话侦测逾时时间(秒)，默认值为 30 秒。于此设置秒数之后重新测试对外会话。

当线路连接失败时： 线路连接失败时的处理方式，有两种：

（1）仅记录到日志：当侦测到与运营商连结失败时，系统就会在系统日志中将这项错误信息纪录下来，但保持此线路不会移除，所以会导致有些原来使用此条线路上的用户无法正常使用。

此选项适用在当某条广域网会话失败时，从这个广域网去访问的目的地地址是无法从另一条线路去访问的时候，就可以用此选项。例如若是要访问 10.0.0.1 到 10.254.254.254 时一定要走广域网 1 去访问，而且广域网 2 是无法访问到此网段，那就可以使用此选项。因为若广域网 1 掉线后走广域网 2 也无法去访问到 10.0.0.1 到 10.254.254.254，就不需要在广域网 1 断线时将此线路移除。

（2）纪录到日志并移除该条线路：当侦测到与运营商连结失败时，系统不会在系统日志中将这项错误信息纪录下来，原本使用此 WAN 端的数据包传递会自动转换到另一条广域端口.等到原本断线的广域端口恢复后会自行重新连结，则数据包传递会自动转换回来。

此选项适用在当某条广域网会话失败时，从这个广域网去访问的目的地位置是可以从另一条线路去访问的时候，就要用此选项。如此可以让任何一条广域网断线的时候，另一条可以做备援，将流量转移到还在会话的广域网。

有流量时不进行侦测： 当下载 或 / 与 上传流量超过带宽的百分之（ ）时，表示线路仍在会话运作，不必再一直送出 NSD 侦测要求数据包

侦测以下可回应的服务器：

默认网关： 近端的默认通讯网关位置，如 ADSL 路由器的 IP 地址，此为路由自动填入，所以只须打勾选择是否启用。

> 注意！
> 有部分的 ADSL 线路的网关是不会响应侦测数据包，或是当您是使用光纤盒，或是运营商发给您的是固定的公网 IP，且网关就是在您网吧这端而不是在运营商那端时，此选项不要启动。

运营商 服务器： 运营商端的侦测位置，如运营商的 DNS 服务器 IP 地址等。在设置此 IP 地址时请确认此 IP 地址是可以且稳定快速的得到响应 (建议填入运营商端 DNS IP)。

远程服务器： 远程的网络节点侦测位置，此 Remote Host IP 地址最好也是可以且稳定快速的得到响应(建议填入运营商端 DNS IP)。

DNS 服务器： 网域名称端 DNS 的侦测位置(此字段只许填入网址如“www.hinet.net”，请勿填 IP 地址)。另外，两条 WAN 的此字段不可以填入相同的网址。

确定： 点击此按钮“确认”即会存储刚才所变动的修改设置内容参数。

取消： 点击此按钮“取消”即会清除刚才所变动的修改设置内容参数，此操作必须于确认存储动作之前才会有效。

注意！

在“指定路由”的负载均衡模式下，第一个广域网口会保留给没有指定到其它广域网口的 IP 或应用服务端口(服务端口)经由此广域网(WAN1)进出。因此建议您在此模式下将您的其中一条线路接在第一个广域网口。当您其它的广域网口断线时，而您在线路侦测机制下选择移除有问题线路，流量就会转移到第一个广域网口(WAN1)。此外，若是第一个广域网口(WAN1)断线，则流量会依次转移到其它广域网口，例如转移到 WAN2，WAN2 也断线则转移到 WAN3 等等。

6.2.3 WAN 口协议绑定设置

协议绑定

使用者可将特定的 IP 或特定的应用服务端口(服务端口)经由您限定的 WAN 出去。其它没有做绑定的 IP 或服务器还是会进行广域网的负载平衡。

注意！

在"指定路由"的负载均衡模式下，第一个广域网口(WAN1)是不能被指定的，保留给没有指定到其它广域网口的 IP 或应用服务端口(服务端口)经由此广域网(WAN1)进出。也就是说第一个广域网口(WAN1)不能设置通讯协议绑定的规则，以避免所有的广域网口都被指定有特定的内网 IP、应用服务端口、目的地 IP，导致其它的 IP 或应用服务端口没有广域网口可以使用。

协议绑定

服务端口：所有端口 [TCP&UDP/1~65535]
服务端口新增或删除表
来源IP地址 10 . 10 . 10 . 0 到 0
目的IP地址：0 . 0 . 0 . 0 到
0 . 0 . 0 . 0
接口位置：广域网1
激活：
上移 增加到对应列表 下移
FTP [TCP/21~21]->10.10.10.0~0(0.0.0.0~0.0.0.0)广域网1
删除选中的项目
显示开启表 确定 取消

服务端口： 在此选择欲开启的绑定服务端口，从下拉式选单中可以选择默认列表(如 All -TCP&UDP 0～65535， WWW 为 80～80， FTP 为 21～21 等等)，默认的服务为 All 0～65535。

点击"服务端新增或删除表"按钮可以进入服务端口设置窗口，进行新增或删除选单中默认的服务端口。

来源 IP 地址：	您可以指定特定的内部虚拟 IP 地址的数据包经由特定的广域端口出去。在此填上内部虚拟 IP 地址范围，例如 192.168.1.100 到 150.则 IP 地址 100 到 150 为绑定范围。如果使用者只需要设置特定的服务端口而不需指定特定的 IP 地址， 则在 IP 的字段皆填入 0。您也可以选择 IP 群组的方式来指定来源 IP。关于 IP 群组的设置，请参考（“7.6 IP 群组管理”的说明）。
目的 IP 地址：	在此填上外部固定 IP 地址，例如若有一目标地址 210.11.1.1，要连接此地址的使用者限定只能从广域端口 1 到达此目标地址，则在此填上外部固定 IP 地址 210.11.1.1 到 210.11.1.1。如果使用者要设置一个范围的目的地位置，则填入方式可以为 210.11.1.1 到 210.11.255.254，则表示整组 210.11.x.x 的 Class C 网段都限制走某一条广域网，若只需要设置特定的应用而不需指定特定的 IP 地址，则在 IP 的字段皆填入 0.0.0.0。
接口位置：	选择您所要绑定此条规则在哪一个 WAN 端口。
激活：	启用此规则。
增加到对应列表：	增加此条规则到列表。
删除选中的项目：	删除在服务列表里所选择的规则。
上移 & 下移：	由于每条规则执行的优先级为由列表的最上面那条往下执行，也就是越后面设置的规则会越后执行，所以您可以自行调整每条规则先后执行顺序。
确定：	点击此按钮“确认”即会存储刚才所变动的修改设置内容参数。
取消：	点击此按钮“取消”即会清除刚才所变动的修改设置内容参数，此操作必须于确认存储动作之前才会有效。

注意！

通讯绑定协议所设的规则在安全路由器执行时也有优先级的，由上到下，在列表上最上方那条会先执行，然后依序往下。

<u>显示开启表：</u>

按下”显示开启表”，会出现以下的对话窗口。您可以选择以“优先级”来显示排列的顺序，或是以“接口位置”来显示排列的顺序。点击“刷新”可以重新显示窗口，点击“关闭”将结束这个对话窗口。

◉ 优先级 ○ 接口位置 刷新 关闭

优先级	接口位置	服务端口	来源IP地址	目的IP地址	激活	编辑
1	广域网1	FTP [TCP/21~21]	10.10.10.0~10.10.10.0	0.0.0.0~0.0.0.0	激活	编辑

新增或删除管理服务端口号

若您欲开启的服务端口项目没有在表列中，您可以点击"服务端口新增或删除表"按钮，新增或删除管理服务端口号列表，如以下所述：

服务名称：

通讯协议： TCP

端口范围： 到

增加到对应列表

所有端口 [TCP&UDP/1~65535]
DNS [UDP/53~53]
FTP [TCP/21~21]
HTTP [TCP/80~80]
HTTP Secondary [TCP/8080~8080]
HTTPS [TCP/443~443]
HTTPS Secondary [TCP/8443~8443]
TFTP [UDP/69~69]
IMAP [TCP/143~143]
NNTP [TCP/119~119]
POP3 [TCP/110~110]
SNMP [UDP/161~161]
SMTP [TCP/25~25]
TELNET [TCP/23~23]
TELNET Secondary [TCP/8023~8023]
TELNETSSL [TCP/992~992]
DHCP [UDP/67~67]
L2TP [UDP/1701~1701]

删除选中的项目

确定 取消 关闭

服务端口名称： 在此自定欲开启的服务端口号名称加入列表中，如 BT 等。

通讯协议： 在此选择欲开启的服务端口号的数据包格式为 TCP 或 UDP。

服务端口的位置范围： 填入您将新增加的服务端口范围。

增加到对应列表： 增加到开启服务项目内容列表，最多可新增 100 组。

删除选中的项目： 删除所选择的开启服务项目内容。

确定： 点击此按钮“确认”即会存储刚才所变动的修改设置内容参数。

取消： 点击此按钮“取消”即会清除刚才所变动的修改设置内容参数，此操作必须于确认存储动作之前才会有效。

关闭： 离开并关闭此功能设置窗口。

使用“智能型”负载均衡模式时其通讯协议绑定协议设置方式：

智能负载均衡方式搭配“通讯协议绑定”可以有更弹性运用您的带宽，您可将特定的内网 IP，使用特定应用服务端口作访问，或特定的目的地 IP 经由您指定的广域网来访问外网。

<u>范例一：若要指定内网 IP 192.168.1.100 去外网访问都走广域网 2，那通讯协议绑定设置方式?</u>

如以下范例所示，服务端选择“所有端口”，在来源 IP 地址填入 192.168.1.100 到 100，目的 IP 地址保留原本的数值 0.0.0.0 (表示所有的外网地址)。接口位置选则广域网 2，然后勾选激活。最后点击“新增”即可将此规则加入。

协议绑定

服务端口：所有端口 [TCP&UDP/1~65535]
服务端口新增或删除表
来源IP地址 192 . 168 . 1 . 100 到 100
目的IP地址：0 . 0 . 0 . 0 到
0 . 0 . 0 . 0
接口位置：广域网2
激活：☑
上移 更新特殊应用软件 下移
所有端口 [TCP&UDP/1~65535]->192.168.1.100~100(0.0.0.0~0.0.0.0)广域网2
删除选中的项目 新增
显示开启表 确定 取消

<u>范例二:若要指定内网 IP192.168.1.150 到 200 去外网访问 80 端口都走只能走广域网 2 去访问，那通讯协议绑定怎样设置?</u>

如以下范例所示，服务端选择“HTTP[TCP/80~80]”，在来源 IP 地址填入 192.168.1.150 到 200，目的 IP 地址保留原本的数值 0.0.0.0 (表示所有的外网地址)。接口位置选则广域网 2，然后勾选激活。最后点击“新增”即可将此规则加入。

协议绑定

<u>范例三：若要指定内网所有 IP 去外网访问 80 端口都走只能走广域网 2，但其余服务都走广域网 1 时，通讯协议绑定是怎样设置?</u>

如以下范例所示，要设置两条规则：

第一条规则服务端选择“HTTP[TCP/80~80]”，在来源 IP 地址填入 192.168.1.0 到 0(表示所有的内网地址)，目的 IP 地址保留原本的数值 0.0.0.0 (表示所有的外网地址)。接口位置选则广域网 2，然后勾选激活。最后点击“新增”即可将此规则加入。QoS 安全路由器会将所有用 80 端口去外网访问的流量都走广域网 2，但是不是用 80 端口的流量根据路由器的自动负载平衡演算，还是有可能会走广域网 2，因此还需要再设第二条规则。

第二条规则，服务端选择“所有端口[TCP&UDP/1~65535]”，在来源 IP 地址填入 192.168.1.2 到 254，目的 IP 地址保留原本的数值 0.0.0.0 (表示所有的外网地址)。接口位置选则广域网 1，然后勾选激活。最后点击“新增”即可将此规则加入。这时 QoS 安全路由器会将不是用 80 端口去外网访问的流量都走广域网 1。

协议绑定

服务端口：HTTP [TCP/80~80]

服务端口新增或删除表

来源IP地址 192 . 168 . 1 . 0 到 0

目的IP地址：0 . 0 . 0 . 0 到

0 . 0 . 0 . 0

接口位置：广域网2

激活：☑

上移 更新特殊应用软件 下移

HTTP [TCP/80~80]->192.168.1.0~0(0.0.0.0~0.0.0.0)广域网2
所有端口 [TCP&UDP/1~65535]->192.168.1.2~254(0.0.0.0~0.0.0.0)广域网1

删除选中的项目 新增

显示开启表 确定 取消

使用“指定路由”的负载均衡模式时其通讯协议绑定协议设置方式：

指定路由的模式让您对特定的内网 IP、特定要访问的应用服务端口或特定目的地 IP 经由您指定的广域网对外网做访问。且一经指定后，该广域网也只能让这些指定的内网 IP、特定要访问的应用服务端口、或特定目的地 IP 使用。其它不在这些指定内的内网 IP、特定要访问的应用服务端口或特定目的地 IP 都会从另一条广域网出去访问。此模式必须配合“通讯协议绑定”功能才能发挥作用。

<u>范例一：若要指定内网所有 IP 去外网访问 80 端口都走只能走广域网 2，但其余服务都走广域网 1 时，通讯协议绑定设置方式是怎样设置?</u>

如以下范例所示设置规则，服务端选择“HTTP[TCP/80~80]”，在来源 IP 地址填入 192.168.1.0 到 0(表示所有的内网地址)，目的 IP 地址保留原本的数值 0.0.0.0 (表示所有的外网地址)。接口位置选则广域网 2，然后勾

选激活。最后点击“新增”即可将此规则加入。此时广域网 2 只会有访问外网 80 端口的流量，其余流量都只走广域网 1。

协议绑定

服务端口：HTTP [TCP/80~80]
服务端口新增或删除表
来源IP地址 192 . 168 . 1 . 0 到 0
目的IP地址：0 . 0 . 0 . 0 到
0 . 0 . 0 . 0
接口位置：广域网2
激活：☑
上移 更新特殊应用软件 下移
HTTP [TCP/80~80]->192.168.1.0~0 (0.0.0.0~0.0.0.0)广域网2
删除选中的项目 新增
显示开启表 确定 取消

<u>范例二：若要指定内网所有 IP 去外网访问 IP 211.1.1.1 到 211.254.254.254 还有 60.1.1.1 到 60.254.254.254 整组 A 类段时都走走广域网 2 去访问，但去其余不是这几个目的地 IP 段时都走广域网 1 时，那通讯协议绑定设置方式如何设置?</u>

如以下范例所示设置两条规则：

第一条规则中服务端选择“所有端口[TCP&UDP/1~65535]”，在来源 IP 地址填入 192.168.1.0 到 0(表示所有的内网地址)，目的 IP 地址填入 211.1.1.1 到 211.254.254.254。接口位置选则广域网 2，然后勾选激活。最后点击“新增”即可将此规则加入。

第二条规则中服务端选择“所有端口[TCP&UDP/1~65535]”，在来源 IP 地址填入 192.168.1.0 到 0(表示所有的内网地址)，目的 IP 地址填入 60.1.1.1 到 60.254.254.254。接口位置选则广域网 2，然后勾选激活。最后点击“新增”即可将此规则加入。此时，除了上述两条规则所涵盖的目的 IP，其余去外网访问的流量都只走广域

网 1。

协议绑定

服务端口：所有端口 [TCP&UDP/1~65535]

服务端口新增或删除表

来源IP地址 10 . 10 . 10 . 0 到 0

目的IP地址：0 . 0 . 0 . 0 到

0 . 0 . 0 . 0

接口位置：广域网2

激活：

上移 增加到对应列表 下移

所有端口 [TCP&UDP/1~65535]->192.168.1.0~0(211.1.1.1~211.254.254.254)广域网2
所有端口 [TCP&UDP/1~65535]->192.168.1.0~0(60.1.1.1~60.254.254.254)广域网2

删除选中的项目

显示开启表 确定 取消

6.2.4 虛擬遶徑 用戶端(未来支持)



虚拟绕径

☑ **激活**

绑定接口位置：	Wan1	
绑定服务网段：	网通网段	重新导入网段
绑定服务端口：	All	重新导入端口
	当连接中断后, 每隔 30 分钟重拨	
远程服务器IP地址：	0 . 0 . 0 . 0	
用户名：		
密码：		
状态：		

确定 取消

激活虚拟遶径功能	勾选此选项,开启虚拟策略路由功能
绑定接口位置	选择虚拟遶径绑定的广网域 WAN 口
绑定服务网段	在此选择设置预走虚拟路由的网域，可选择网通或是自定义。这里您可以根据实际需要自己设置绑定的网域。
重新导入网段	点此按钮修改虚拟策略路由 IP 段，点击浏览汇入自定义 IP 文件。（自定义 IP 文件的编写见此表后文件编写 1）
绑定服务端口	在此选择设置预走虚拟路由的端口，可选择所有端口、游戏端口或是自定义。这里您可以根据实际需要自己设置绑定的服务端口。
重新导入端口	点此按钮修改虚拟策略路由服务端口，点击浏览汇入自定义端口文件。（自定义端口文件的编写见此表后文件编写 2）
当连接中断后,每隔 30 :	此处填写当虚拟绕径中断连接时,重新尝试再次连接的时间间隔,默认为 30 分钟。您可以根据需要填入自定的时间间隔。

分钟重拨	
远程服务器 IP 地址	在此填写虚拟遂径服务器的外部 IP 地址。
用户名称	在此输入虚拟遂径使用者的名称。
密码	在此输入虚拟遂径服务器的密码。
状态	显示虚拟路由连接状态：联机或掉线

文件编写 1——自定义 IP 文件

自定义 IP 文件的建立可以用纯文本编辑软件来撰写，例如使用 Windows 系统自带的文本编辑程序“记事本”来建立。将您要指定的目的 IP 地址按照下图的格式写入。例如您要指定的目的 IP 地址范围是从 140.115.1.1 到 140.115.1.255，则在“记事本”中输入 140.115.1.1～140.115.1.255。下一个目的 IP 地址范围则要换行输入。请注意！若是只有一个目的 IP 地址，也需要以同样的格式来书写。例如指定的目的 IP 地址是 210.66.161.54，则必须写成 210.66.161.54～210.66.161.54 格式。存储文件后(扩展名应该是.txt)即可汇入修改虚拟策略路由 IP 段。



文件编写 2——自定义端口文件

自定义 IP 文件的建立可以用纯文本编辑软件来撰写，例如使用 Windows 系统自带的文本编辑程序“记事本”来建立。将您要指定的端口按照下图的格式写入，例如您要指定 TCP/3724~3724 端口，则在“记事本”中输入 TCP/3724~3724。下一个指定端口则要换行输入。存储文件后(扩展名应该是.txt)即可汇入修改虚拟策略路由服务端口。



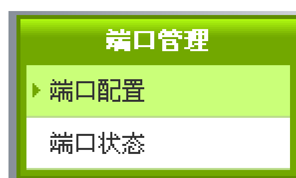
TCP/3724~3724
UDP/15850~15851
TCP/15779~15779
TCP/9801~9801
TCP/38888~38888
TCP/13000~13001
TCP/5816~5816
TCP/16188~16188
TCP/6299~6299
TCP/7600~7900
TCP/9010~9012
TCP/11002~11008
TCP/6020~6020

七、内部局域网络设置

通过本章节可以对端口进行设置管理，了解如何设置内部局域网络的 IP 地址。

7.1 网络端口管理设置

管理者可以设置网络实体联机于每一个以太网络端口，如连接速率，工作模式，优先级，自动翻转或是 VLAN 等以太网络端口的功能。



端口设置

☑ 激活端口1为端口镜像

端口号	端口	关闭端口	优先权	网络端口连接速率	半双/全双工模式	自动侦测模式	VLAN
1	局域网	☐	高级	○ 10M ◉ 100M	○ 半双 ◉ 全双	☑ 激活	VLAN1
2	局域网	☐	高级	○ 10M ◉ 100M	○ 半双 ◉ 全双	☑ 激活	VLAN2
3	局域网	☐	高级	○ 10M ◉ 100M	○ 半双 ◉ 全双	☑ 激活	VLAN3
4	局域网	☐	高级	○ 10M ◉ 100M	○ 半双 ◉ 全双	☑ 激活	VLAN4
5	广域网1	☐	高级	○ 10M ◉ 100M	○ 半双 ◉ 全双	☑ 激活	
6	广域网2	☐	高级	○ 10M ◉ 100M	○ 半双 ◉ 全双	☑ 激活	

*此为示意图，会因产品线不同，图形会有所差异

镜像端口：勾选"激活镜像端口（Port 1）"可以将局域网的第一个端口设置为镜像端口，所有从内网到外网访问的流量都会复制到镜像端口。因此您可以将监控或是过滤服务器直接接在镜像端口，来达到监控或是过滤网络数据包的目的。一旦您激活这个功能，首页中的"端口设置状态"会显示端口 1 为"镜像端口"。如下图：

端口配置状态

端口号	1	2	3	4
接口位置	镜像端口	局域网		
状态	激活	激活	激活	激活

端口号	Internet	Internet
接口位置	广域网1	广域网2
状态	连接	激活

*此为示意图，会因产品线不同，图形会有所差异

关闭端口： 此为设置以太网络的 LAN 端口开启或是关闭的功能，若是打勾的话，则此以太网络端口立即被关闭无法连接使用。默认为开启无打勾。

优先级设置： 此为设置此以太网络的 LAN 端口数据包传送优先权设置，若是此端口设置为高的话，则最优先使用传送数据包的权利，默认优先级为一般。

网络端口连接速度： 此为设置此以太网络的端口网络实体连接速率选项，您可以设置为 10Mbps 或是 100Mbps 连接速度。默认为自动侦测。

半双/全双工模式： 此为设置此以太网络的端口网络实体连接速率工作模式选项，您可以设置为半双工模式或是全双工模式运作。默认为自动侦测。

自动翻转功能： 此为设置以太网络的端口网络实体连接速率自动侦测模式，若是勾选的话，自动侦测所有连接端口的信号与调整。

VLAN： 此功能可以让网管人员在自己的局域网内将每一个局域网端口设置 1 个或多个不同网段且无法互通的局域网端口，但都可以通过 QoS 安全路由器上网络。在同一个网段内的成员(在同一个 VLAN 局域网络内)可互相沟通并看得到对方，若不在同一个 VLAN 群组内的成员则无法得知其它成员的存在。使用者可为每一个 LAN 端口选定为哪一个 VLAN 局域网络群组。

VLAN All： 当网管人员在内网设置了多个 VALN 端口，且不在同一个 VLAN 群组内无法互访，可是内网又需要架设服饰器让内网所有 VLAN 群组都可以访问此服务器，此时可以将某一局域网端口设置为 VLAN All，将此服务器接入此 VLAN All 的端口，这样就可以让所有不同 VLAN 群组的计算机都可以访问到此服务器。

7.2 网络端口状态实时显示

此项功能可以让网络管理者查看每个实体端口的详细信息。

端口号：1

摘要信息

网路连接状态	10Base-T / 100Base-TX / 1000Base-T
接口位置	局域网
线路连线状态	关闭
端口配置状态	端口激活
优先级设定	一般
连接速率	10 Mbps
半双/全双工模式	半双工
自动翻转功能	激活
VLAN	VLAN1

流量实时状态

接收数据包统计	0
数据包接收Byte数量	3052672
传送数据包统计	0
数据包传送Byte数量	3204100
错误数据包统计	0

刷新

整体资讯项目：

网路连接状态（10Base-T / 100Base-TX / 1000Base-T），接口位置（局域网/广域网络/DMZ），线路连线状态(激活/关闭)，端口设置状态（端口激活/端口关闭），优先级设置（高级/一般），网路连接速率（10Mbps/100Mbps/1000Mbps)，半双/全双工模式(半双工/全双工)，自动翻转功能（激活/关闭），VLAN（VLAN Number / VLAN All）。

端口流量实时状态：

即时显示安全路由器工作状态下的接收和传送数据包计算、数据包接收和传送 Byte 数以及错误数据包统计实际数值。

7.3 DHCP 发放 IP 服务器

安全路由器的 DHCP 服务器，默认值是启动，可以提供局域网络内的计算机自动取得 IP 的功能，(如同 NT 服务器中的 DHCP 服务)，好处是每台 PC 不用去记录与设置其 IP 地址，当计算机开机后，就可从安全路由器自动取得 IP 地址，管理方便。

IP/DHCP 配置
- DHCP 配置
- DHCP 状态
- IP与MAC绑定
- IP 群組管理

☑ 激活 DHCP服务器

DHCP 用户使用IP范围

租约到期时间 1440 分钟

起始IP地址：10.10.17.100
结束IP地址：10.10.17.149

域名解析服务(DNS)

DNS 服务器(首选) 1:	0.0.0.0
DNS 服务器(备用) 2:	0.0.0.0

WINS服务器

WINS服务器地址:	0.0.0.0

确定 取消

动态 IP 服务：

租约时间： 此设置为发给 PC 端 IP 地址的租约时间，默认为 1440 分钟(代表时间为一天)，当租约时间到后，PC 端会重新跟路由再申请一次。您可以依照实际需求来设置。

起始 IP 地址： 系统默认为四个网段从 192.168.1.100、192.168.2.100、192.168.3.100、192.168.4.100 的 IP 地址开始发放。您可以依照实际需求来设置。

结束 IP 地址： 系统默认为四个网段 192.168.1.149、192.168.2.149、192.168.3.149、192.168.4.149IP 地址为最后发放 IP，也就是说出厂设置值每个网段可供 50 台计算机自动取得 IP 地址，四个网段共 200 台计算机自动取得 IP 地址。您可以依照实际需求来设置。

域名解析服务（DNS）地址：

此设置为发给 PC 端 IP 地址的 DNS 网域服务器查询地址，若您有特定使用的 DNS 服务器，可以直接输入此服务器的 IP 地址，则 PC 端从 DHCP 取得 IP 地址时，也会一并取得指定的 DNS 服务器地址。

DNS 服务器 (首选) 1： 输入 DNS 网域服务器的 IP 位置。

DNS 服务器 (备用) 2： 输入 DNS 网域服务器的 IP 位置。

WINS 服务器：

若您的网络上有解析 Windows 计算机名称的服务器，您可以直接输入此服务器的 IP 地址。

WINS 服务器地址： 输入 WINS 网域服务器的 IP 位置。

确定： 点击此按钮"确认"即会存储刚才所变动的修改设置内容参数。

取消： 点击此按钮"取消"即会清除刚才所变动的修改设置内容参数，此操作必须于确认存储动作之前才会有效。

7.4 DHCP 状态显示

此状态表为显示 DHCP 服务器的目前使用状态与设置纪录等，以便提供管理人员需要时做网络设置参考数据。

状态

DHCP服务器：	10.10.10.1
已使用的动态IP数量：	0
已发放的固定IP数量：	0
剩余可用的IP数量：	50
可发放的IP总量：	50

DHCP 用户连接列表

主机名称	IP地址	MAC地址	租约到期时间	删除

刷新

DHCP 服务器 IP 地址: 目前 DHCP 服务器的 IP 地址。

已使用的动态 IP 数量： 目前 DHCP 服务器已经发放动态 IP 的数量。

已发放的固定 IP 数量: 目前 DHCP 服务器已经发放固定 IP 的数量。

剩余可用的 IP 地址: 目前 DHCP 服务器可以还可发放的 IP 数量。

可发放的 IP 总量: 目前 DHCP 服务器所设置可发放的 IP 总数量。

主机名称: 目前此台计算机的名称。

IP 地址: 目前此台计算机所取得的 IP 地址。

MAC 地址: 目前此台计算机的 MAC 网络实体位置。

租约到期时间: DHCP 目前核发 IP 地址的租约时间。

删除: 删除此笔核发 IP 纪录。

DNS 自订资料库

一般网络应用是将 DNS 服务器指向外部运营商的 DNS 服务器，或内部自行架设的 DNS 服务器，现在侠诺的安全路由器也提供类似「简易」的自订 DNS 服务，称为「DNS 自订资料库」，可以将网域名称与该名称所对应的 IP 地址做简单的设置。

DNS 自订资料库

主机名称： (Ex: www.google.com)

IP地址：

增加到对应列表

erp.com => 10.10.10.2
jay => 10.10.10.222
www => 119.160.246.241
www.msn.com.tw => 59.124.180.50
tw.yahoo.com => 10.10.10.199

删除选中的项目

主机名称：	输入需要做解析对应的网域名称。例如 www.google.com。
IP 地址：	输入上述网域名称所对应的 IP 地址。
加入到对应列表：	将输入好的网域名称与 IP 对应，加入到下方对应列表当中。
删除点选的项目：	删除所选的的对应项目。

※请注意！

(1)「必须」要启用 DHCP 服务器服务，DNS 自订资料库服务才会启用。

(2) 需要使用 DNS 自订资料库，需要将 DHCP 服务器的网域解析服务(DNS) IP 地址输入成防火墙 / 路由器设备的局域网网关 IP，以下图为例，局域网网关 IP 目前是 10.10.10.1。

局域网(LAN)接口配置

MAC地址：	00 - 17 - 41 - 51 - 88 - 45 (默认值: 08-3b-ba-8a-67-b9)
局域网网关：	10 . 10 . 10 . 1
子网掩码：	255 . 255 . 240 . 0

所以 DHCP 的 DNS IP 地址也要设定成 10.10.10.1，DNS 自订资料库的对应效果才会生效（如下图）。

域名解析服务(DNS)

DNS 服务器(首选) 1:	10 . 10 . 10 . 1
DNS 服务器(备用) 2:	0 . 0 . 0 . 0

(3) 启用 DNS 自订资料库后，没有在资料库对应清单中的网域名称，还是会透过外网的运营商 DNS 服务器或是内网自行架设的 DNS 服务器进行解析。

测试 DNS 自订资料库是否生效：

假设设定 tw.yahoo.com 网域名称所对应的 IP 地址 10.10.10.199 如下图：

DNS 自订资料库

主机名称：tw.yahoo.com (Ex: www.google.com)

IP地址：10 . 10 . 10 . 199

更新区块

erp.com => 10.10.10.2
jay => 10.10.10.222
www => 119.160.246.241
www.msn.com.tw => 59.124.180.50
tw.yahoo.com => 10.10.10.199

删除选中的项目　新增

(1) 系统工具 => 自我诊断 => 域名解析测试

◉ 域名解析测试　○ Ping测试

测试域名(www.qno.cn)：　开始

(2) 输入网域名称 tw.yahoo.com 进行查询/解析

◉ 域名解析测试　○ Ping测试

测试域名(www.qno.cn)：tw.yahoo.com　开始

(3) 解析出来的 IP 地址为 10.10.10.199，确认为 DNS 自订资料库所设定的对应 IP

◉ 域名解析测试　　　○ Ping测试

测试域名(www.qno.cn) : tw.yahoo.com 开始
名称: tw.yahoo.com
地址: 10.10.10.199

7.5 IP 及 MAC 地址绑定

在许多的大中型网吧及企业网络中，网管人员可以设置安全路由器所提供的 IP & MAC 绑定功能，达到用户不能自行添加计算机来使用对外网络或是私自擅改 IP 上网影响他人。另外通过此功能也可以将每台计算机或服务器的 MAC 地址绑定，达到计算机或服务器每次开机或重新要 IP 时，都分配给它相同的一组 IP 地址。



IP与MAC绑定

显示新加入的IP地址

静态IP地址：

所对应的MAC地址：

名称：

激活：

增加到对应列表

删除选中的项目

封锁绑定列表中IP地址与MAC地址不对应的用户

封锁未绑定或绑定列表中未激活的用户

显示开目表 确定 取消

您可以以两种方式来设置这个功能：

(一)限定可以使用网络的 MAC 地址

此功能主要目的是限制只有在列表里面的 MAC 地址才可以得到 DHCP 分配的 IP 地址上网，未在此列表的计算机都无法取得 IP 上网；或是限制有在列表但是未激活绑定功能的计算器。当使用此功能时，切记要将静态 IP 地址填 0.0.0.0 不可以空白，另外将"封锁未绑定或绑定列表中未激活的用户"选项勾选才可以执行。如下图中范例所示：

IP与MAC绑定

显示新加入的IP地址

静态IP地址 : . . .
所对应的MAC地址 : - - - - -
名称 :
激活 : ☐
增加到对应列表

删除选中的项目

☐ 封锁绑定列表中IP地址与MAC地址不对应的用户
☑ 封锁未绑定或绑定列表中未激活的用户

显示开启表 确定 取消

(二)IP 及 MAC 地址绑定

此功能主要目的是让指定的 MAC 地址计算机在每次开机都会要到同一个指定 IP。此外，若将"封锁绑定列表中 IP 地址与 MAC 地址不对应的用户" 功能启用，那么设置为固定 IP 的计算机或通过此功能已发给特定 IP 的计算机擅自更改 IP 为非指定的 IP 地址时，则会无法上网。

IP与MAC绑定

显示新加入的IP地址

静态IP地址 : . . .

所对应的MAC地址 : - - - - -

名称 :

激活 :

增加到对应列表

删除选中的项目

☑ 封锁绑定列表中IP地址与MAC地址不对应的用户

☑ 封锁未绑定或绑定列表中未激活的用户

显示开目表 确定 取消

静态 IP 地址设置：	此字段有两种填入方式： 1. 若您只要限制 MAC 地址可以跟 DHCP 要 IP 而不一定是指定的那一个 IP，请在此字段填 0.0.0.0，不可为空白。 2. 若要求每次此台计算机都要分配到同一个 IP，则将您所要求分配给此台计算机的 IP 地址输入。这样所要绑定服务器或 PC 端每次重启都会要到固定的同一个虚拟 IP。
所对应的 MAC 地址:	输入要绑定的服务器或 PC 端固定实体 MAC(网络卡上的地址)。
名称:	填入您所绑定此用户的名字或地址做辨识，可输入 12 个字符，中英文皆可以。
激活:	启用此组设置。
增加到对应列表:	增加或修正此设置到列表中。
删除选中的项目:	删除列表中所选择的绑定。
新增:	当列表中有绑定规则后，右下角会出现此按钮，可点击增加新的绑定。

封锁绑定列表中 IP 地址与 MAC 地址不对应的用户: 此选项打勾后，只要是 User 自行更改计算机的 IP 或不是列表设置的 IP 将无法上网。

封锁未绑定或绑定列表中未激活的用户: 此选项打勾后，只要不在列表中或是在列表中未激活绑定功能的 MAC 地址都无法上网。

显示出还未做绑定或新加入的 IP 及其 MAC 地址：

此功能的主要目的是为了减少网管人员需一一查询每台计算机的 MAC 地址后才能进行绑定，因为会非常耗时且困难。再者，将 MAC 地址手动填入列表也很容易出错。所以只需要查询此表格，就可以看到所有进出 QOS 安全路由器且还未绑定的 MAC 地址，然后直接在此表格做绑定动作即可。另外，若您发现此表格出现已经绑定的某组 MAC 又出现在此表格，则表示此用户试图修改不是您指定的 IP 上网。

新加入的IP 地址列表 - Windows Internet Explorer

http://220.130.188.40/Dhcp_table1.htm

确定 全选 刷新 关闭

IP地址	MAC地址	名称	激活
10.10.10.104	00:17:16:01:f0:b2		
10.10.10.103	00:17:16:01:66:b3		
10.10.10.101	00:0e:a0:00:1d:a3		
10.10.10.100	00:01:80:37:fb:c3		
10.10.10.107	00:1b:24:d1:af:15		
10.10.10.105	00:17:16:00:a6:68		
10.10.10.106	00:17:16:00:c6:8b		
10.10.10.100	00:11:2f:5a:ac:9c		
10.10.10.102	00:17:16:01:94:3e		

完成 網際網路 100%

名称: 可以填入您所绑定此用户的名字或地址做辨识，可输入 12 个字符。

激活 勾选您所要绑定的目标。

确定: 将您所选定好的目标绑定到 IP & MAC 绑定列表。

全选 选择所有在此列表中的目标做绑定。

刷新： 更新此列表。

关闭: 关闭此列表。

7.6 IP 与服务通讯端口群组管理

IP 群组功能可以让您将数个 IP 地址或 IP 地址范围组合成一个群组。当您以 IP 地址来管理使用者的网络存取权限的时候，您可以将具有相同使用权限的使用者设定在同一个 IP 群组里，并在各个管理功能中选择以 IP 群组的方式来做设定，可以减少以单一 IP 来做设定的规则数。例如在“通讯协议绑定”的设定，“带宽管理(QoS)”的设定，以及“访问规则”的设定中，都可以选择以 IP 群组的方式来做设定，如此就不需要再以单一 IP 来设定，减少所需要的规则数。

IP 群组有分成本地 IP 群组与远程 IP 群组，本地群组是指局域网内的来源 IP 群组，远程群组是指广域网外的目的地 IP 群组；本地群组的用户 IP 编辑清单，会自动学习有流量经过防火墙的 IP 地址，并且如果用户更动 IP，清单内的 IP 也会跟着变动，但是已经加入群组的 IP 数据，不会随着左方 IP 清单的改变而自动变更群组内容，必须由管理使用者手动进行更改。

用户IP编辑

名称:

IP地址: . . . 到

加入IP列表

IP列表

name	IP	delete
	192.168.1.103	

>>>>

本地群组配置

IP群组 : test

新增群组

删除群组

群组名称 : test

name	IP	delete
	192.168.1.100~100	
	192.168.1.2~2	

確定 取消

用户 IP 编辑: 除了原本在左下方就会出现的自动学习 IP 清单，也可以自行手动设定 IP 地址。

名称： 输入下方输入 IP 地址 (或范围) 所代表的名称。

IP 地址： 输入 IP 地址 (或范围) 内容。例如 192.168.1.200 到 250。

加入 IP 列表： 设定完 IP 地址的名称与内容后，按下此按钮将数据加入下方 IP 列表，若此 IP (或范围) 已在列表中是无法加入的。

本地群组设定： 设定本地 IP 群组，可以直接从左方的 IP 清单中拉选成 IP 群组组合。

IP 群组： 在此字段选择您要修改的 IP 群组内容名称，若是要新增群组，请按下旁边的「新增群组」按钮。

群组名称： 会在此字段显示群组名称内容，在新增群组的时候，也请注意要输入群组名称在该字段中。

删除群组： 从下拉式选单选择欲删除的群组内容，并按下「删除群组」按钮，此时系统会再确认一次是否删除该群组，按下确认后就会删除该群组内容。

>>>> 按钮： 可以由左方 IP 清单一次点选多个 IP 后，按下此按钮加入右方的群组内容清单中。

delete： 将自定义的 IP 或是 IP 范围进行删除。

确定： 点击此按钮"**确认**"即会存储刚才所变动的修改设定内容参数。

取消： 点击此按钮"**取消**"即会清除刚才所变动的修改设定内容参数，此操作必须于"确定"存储动作之前才会有效。

远程 IP 组管理：

基本上远程 IP 组设定的方式与本地 IP 组管理设定方式完全相同，但由于是远程 IP，所以并没有自动学习功能，并需自己手动定义远程的 IP 地址、范围与群组，例如 220.130.188.1 到 200 (范围)。

用户IP编辑
名称:
IP地址: . . . 到
加入IP列表

IP列表

name	IP	delete

\>>>>

远端群组配置
IP群组：
新增群组
删除群组

群组名称：

name	IP	delete

设定方式一样也是设定好左方单一远程 IP 地址或范围的内容后，于右方设定拉选要加入某群组的 IP 地址数据。

7.7 服务通讯端口 群组管理

除了 IP 地址可以成为群组设定外，服务埠也可以群组起来，方便对于 QoS、防火墙访问规则设置等功能的设定。

用户端口编辑

名称：

通讯协定：TCP

服务端口范围：到 加到端口列表

端口列表

name	protocol	port	delete
All Traffic	BOTH	1~65535	
DNS	UDP	53~53	
FTP	TCP	21~21	
HTTP	TCP	80~80	
HTTP Secondary	TCP	8080~8080	
HTTPS	TCP	443~443	
HTTPS Secondary	TCP	8443~8443	
TFTP	UDP	69~69	
IMAP	TCP	143~143	
NNTP	TCP	119~119	
POP3	TCP	110~110	
SNMP	UDP	161~161	
SMTP	TCP	25~25	

››››

端口群组配置

群组： 新增群组 删除群组

群组名称：

name	protocol	port	delete

用户端口编辑: 针对所需的服务埠手动进行设定，依序为名称、通讯协议、服务端口范围。

名称： 将此服务端口命名以识别其属性。例如：Virus135

通讯协议： 设定服务埠属于 TCP 或 UDP 或 TCP&UDP 那种通讯协议。

服务端口范围： 设定服务埠 (Port) 范围。例如 135 到 135

加到端口列表： 设定服务端口的名称、通讯协议与端口范围后，按下此按钮就会加入到下方的埠列表，并且此埠可以成为某个埠群组的内容。

群组名称： 会在此字段显示端口群组名称内容，在新增群组的时候，也请注意要输入群组名称在该字段中。例如 Virus。

删除群组： 从下拉式选单选择欲删除的群组内容，并按下「删除群组」按钮，此时系统会再确认一次是否删除该群组，按下确认后就会删除该群组内容。

›››› 按钮： 可以由左方服务端口清单一次点选多个服务端口后，按下此按钮加入右方的群组内容清单中。

delete：	将自定义的服务埠或是服务埠范围进行删除。
确定：	点击此按钮“**确认**”即会存储刚才所变动的修改设定内容参数。
取消：	点击此按钮“**取消**”即会清除刚才所变动的修改设定内容参数，此操作必须于“确定”存储动作之前才会有效。

八、QoS 带宽管理功能

带宽管理 QoS 为 Quality of Service 缩写，其功能主要为限制某些服务及 IP 的带宽使用量，以满足特定应用程序或服务所需要的带宽或优先权，并让其余的使用者共享带宽，才能有比较稳定、可靠的数据传送服务。网络管理人员应该针对网吧、企业等的实际需求，对各种不同网络环境、应用程序或服务来进行带宽管理，才能充分且有效率的达到网络带宽使用。

8.1 带宽设置(QoS)

ISP实际可用带宽

接口位置	上传带宽 (Kbit/sec)	下载带宽 (Kbit/sec)
广域网1	10000	10000
广域网2	10000	10000

QoS带宽管理

控制类型： ⦿ 带宽控制 ○ 优先级

接口位置： ☐ 广域网1 ☐ 广域网2

服务端口： 所有端口 [TCP&UDP/1~65535]

服务端口新增或删除表

IP地址 : 10 . 10 . 10 . 0 到 0

目的： 上传

保证带宽： Kbit/sec 最大可用带宽： Kbit/sec

带宽分配方式： ⦿ 此范围每一IP地址独享此设定带宽.
○ 此范围所有IP地址共享此设定带宽.

激活： ☐

上移 增加到对应列表 下移

删除选中的项目

☐ 激活动态智能QoS

显示开目表 确定 取消

*此为示意图，会因产品线不同，图形会有所差异

8.1.1 带宽设置

ISP实际可用带宽

接口位置	上传带宽 (Kbit/sec)	下载带宽 (Kbit/sec)
广域网1	10000	10000
广域网2	10000	10000

*此为示意图，会因产品线不同，图形会有所差异

WAN 的带宽数据请填入您所申请的宽带网络实际上传及下载带宽，QoS 的带宽控制会依照您所填入的带宽作为计算依据。例如每个 IP 及服务端口（服务端口）可以保障使用的上传或下载的最小带宽会依照此 WAN1 及 WAN2 的实际带宽相加来换算实际可保障的大小。例如上传带宽若两条都为 512Kbit/Sec，那实际上传带宽就为 WAN1+WAN2=1024Kbit/Sec，所以若有 50 个 IP 在内部网络，若要保证每人最小可使用的上传带宽，则就把 1024Kbit/50=20Kbit，这样每人可以保证的最小带宽就可以填 20kbit/Sec，下载同此换算方式。

注意！

这里的数值单位是 kbit，有些应用软件显示下载/上传速度单位为 KB，两个数值之间的换算方式为 1KB=8kbit。

8.1.2 QoS 设置

QoS 可以选择两种方式，无法同时使用，一为流量控制(带宽管理)，另一个为优先权控制，设置人员可以依照自己内网需求做两种模式灵活运用。

带宽控制 (带宽管理) - 依使用量做管理：

网管人员可依照您现有的带宽大小做每一个 IP 或一个范围的 IP 的使用量限制或保障带宽。另外也可以针对服务端口去做带宽控制。若是内部有架设服务器的话，也可控制或保障其对外带宽。

QoS带宽管理

控制类型： ◉ 带宽控制 ○ 优先级

接口位置： ☐ 广域网1 ☐ 广域网2

服务端口： 所有端口 [TCP&UDP/1~65535]

服务端口新增或删除表

IP地址 : 10 . 10 . 10 . 0 到 0

目的： 上传

保证带宽： Kbit/sec 最大可用带宽： Kbit/sec

带宽分配方式： ◉ 此范围每一IP地址独享此设定带宽. ○ 此范围所有IP地址共享此设定带宽.

激活： ☐

上移 增加到对应列表 下移

删除选中的项目

*此为示意图，会因产品线不同，图形会有所差异

接口位置： 勾选此条 QoS 设置要控制在哪条 WAN 执行，可单独或全部勾选。

服务端口： 选择此条 QoS 所要设置的带宽控制为哪个，若您是要针对每个 IP 的所有服务的使用带宽，则将此选择在 All(TCP&UDP)1~65535。若您只要针对譬如 FTP 上传或下载，其余服务不限制，则选择 FTP Port21~21，可参考服务号码默认列表。

IP 地址：

此为选择您所要限制的使用者为哪些?若您只限制单一 IP，则直接将此 IP 填入，如：192.168.1.100 到 100，则此规则就是针对 192.168.1.100 此 IP 做控制。若是要限制一组 IP 范围，则填入如 192.168.1.100 到 150，这样此规则就是针对 192.168.1.100 到 150 做限制。若是此条带宽限制是针对所有人也就是接在 QoS 安全路由器内网的所有 User 则可在 IP 的字段皆填入 0，也就是 192.168.1.0 到 0，这样就表示所有 IP 都受此规则限制。另外此 QoS 是可以控制到 Class C 的范围。

您也可以选择 IP 群组的方式来指定来源 IP。关于 IP 群组的设置，请参考（“5.4 IP 群组管理”的说明）。

目的：

上传： 指对内网 IP 的上传带宽

下载： 指对内网 IP 的下载带宽

虚拟服务器上传(Server in LAN，上传)：若您有架设对外的 Server 网站在 QoS 安全路由器内部，则此选项为控制外部访问此 Server 的带宽控制。

虚拟服务器下载(Server in LAN，下载)：若您有架设网站在 QoS 安全路由器内网，则此选项为控制外部对此服务器上传数据时的带宽控制，例如网吧很多都有架设游戏服务器，若外部要来做此游戏服务器做数据升级时，可以用此控制做带宽管理，才不会影响内部使用者上网打游戏。

保证带宽 & 最大可用带宽：(Kbit/Sec)

保证带宽：此为限制或保证此条规则的最小可使用带宽。

最大可用带宽：此为限制此条规则的最大可使用带宽，也就是最大不会超过此设置值。

请注意！这里填入的数值单位是 kbit，有些应用软件显示下载/上传速度单位为 KB，两个数值之间的换算方式为 1KB=8kbit。

管制时间：

选择“所有时间”，此 QoS 设置在所有时间都有效果，如果选择“从___:___到___:___”填入时间段（24 小时记时制，例如 19：00 到 24：00），以及勾选“每天/周日/周一/周二/周三/周四/周五/周六”的某一天或者几天，其 QoS 设置只在所勾选设置的特定时间段内有效。

带宽分配方式： 此范围每一 IP 地址独享此设置带宽：

若选择此规则的话，其表示每一个 IP 或这一段服务端口都可以有此保证带宽到最大可用带宽)带宽范围，例如若是针对每台计算机 (IP 地址)做的规则设置，则每台计算机(IP 地址)都可以有这么大的带宽。

此范围所有 IP 地址共享此设置带宽：

若选择此规则的话，其表示所有 IP 或此服务端口共享这段(保证带宽到最大可用带宽)带宽范围。

请注意！当您选择带宽的共享方式时，要留意实际应用的情况，以避免选择不恰当的方式而造成带宽太小无法正常使用网络。例如，内网多人使用 FTP 做文件下载，若是您希望 FTP 不会占用掉大部分的带宽，您就可以选择共享带宽，不论内网有多少人使用 FTP 做文件下载，总和所占用的带宽是固定的。

激活： 启用此规则。

增加到对应列表： 增加此条规则到列表。

上移 &下移： 由于 QoS 的每条规则执行的优先级为由列表的最下面那条往上执行，也就是越后面设置的规则会优先执行，所以您可以自行调整每条规则先后执行顺序。通常将要限制带宽的服务端口移至最下方如 BT，e-mule 等，然后将针对限制 IP 带宽的规则往上移。

删所选中的项目： 删除在服务列表里所选择的项目内容。

显示开启表： 可以显示出您所有在带宽管理设置的规则，并可直接点击"编辑"做修改（见表后详解）。

确定： 点击此按钮"确认"即会存储刚才所变动的修改设置内容参数。

取消： 点击此按钮"取消"即会清除刚才所变动的修改设置内容参数，此操作必须于确认存储动作之前才会有效。

显示开启表：

点击左下方的"显示开启表"按钮，会出现以下的对话窗口。您可以选择以"规则"来显示已设置的规则，或是以"接口位置"来显示已设置的规则。点击"刷新"可以重新显示窗口，点击"关闭"将结束这个对话窗口。可直接点击"编辑"做修改。

◉ 规则 ○ 接口位置 刷新 关闭

服务端口	IP地址	目的	保证带宽 (Kbit/sec)	最大可用带宽 (Kbit/sec)	带宽分配方式	激活	接口位置	编辑

范例一：若希望内网去做 ftp 下载(ActiveMode)都只能共同使用 50kbit 下载带宽要如何设置?

以 2WAN 路由器产品为例，接口位置勾选广域网 1、2，服务端选择“ FTP[TCP /21~21”，在 IP 地址填入 0.0.0.0 到 0(表示所有的地址)，目的选择下载。最小带宽填入 2 kbit/sec，表示 FTP 下载保证有 2kbit/sec 的带宽。最大带宽填入 50kbit/sec，表示 FTP 下载最多只能使用到 50kbit/sec 的带宽。带宽共享方式选择“此 IP 地址共享此设置带宽”，如此不管内网有多少人使用 FTP，不论哪个广域网接口，FTP 下载的带宽总和最多只能使用 50kbit/sec。勾选激活，最后点击“新增”即可将此规则加入。

控制类型： ◉ 带宽控制 ○ 优先级

接口位置： ☑ 广域网1 ☑ 广域网2
服务端口： FTP [TCP/21~21]
服务端口新增或删除表
IP地址： 0 . 0 . 0 . 0 到 0
目的： 下载
保证带宽： 2 Kbit/sec 最大可用带宽： 50 Kbit/sec
带宽分配方式： ◉ 此范围所有IP地址共享此设定带宽 ○ 此范围每一IP地址独享此设定带宽
激活： ☑
上移 更新特殊应用软件 下移
FTP [TCP/21~21]->0.0.0.0~0(下载)=>2~50Kbit/sec->广域网1, 2
删除选中的项目 新增

范例二：若希望内网所有 IP 每人最大下载使用带宽只能有 512Kbit，需要一个 IP 一个 IP 设置吗?

不需要一个 IP 一个 IP 设置。以 2WAN 路由器产品为例，接口位置勾选广域网 1、2，服务端选择"No Check Port[TCP&UDP /0~0"，在 IP 地址填入 192.168.1.2 到 254(要作限制的地址范围)，目的选择下载。最小带宽填入 2 kbit/sec，表示每个 IP 保证有 2kbit/sec 的带宽。最大带宽填入 512kbit/sec，表示每个 IP 最多只能使用到 512kbit/sec 的带宽。带宽共享方式选择"此范围每一 IP 地址最大及最小可用带宽"，如此每一个 IP 最小一定有 2kbit/sec 的保证。勾选激活，最后点击"新增"即可将此规则加入。

QoS带宽管理

控制类型： ⊙ 带宽控制 ○ 优先级

接口位置： ☑ 广域网1 ☑ 广域网2

服务端口： Not Check Port[TCP&UDP/0~0]

服务端口新增或删除表

IP地址 ： 192 . 168 . 1 . 2 到 254

目的： 下载

保证带宽： 2 Kbit/sec 最大可用带宽： 512 Kbit/sec

带宽分配方式： ⊙ 此范围每一IP地址独享此设定带宽. ○ 此范围所有IP地址共享此设定带宽.

激活： ☑

上移 更新特殊应用软件 下移

Not Check Port[TCP&UDP/0~0]->192.168.1.2~254(下载)=>2~512Kbit/sec->WAN1, 2

删除选中的项目 新增

范例三：若希望内网所有 IP192.168.1.100-150 每人最大下载使用带宽只能有 1M，但当使用 ftp 下载时 (ActiveMode)都只能共享 512Kbit 时要如何设置?

以 2WAN 路由器产品为例，第一条规则接口位置勾选广域网 1、2，服务端选择"No Check Port[TCP&UDP /0~0"，在 IP 地址填入 192.168.1.100 到 150(要作限制的地址范围)，目的选择下载。最小带宽填入 2 kbit/sec，表示每个 IP 保证有 2kbit/sec 的带宽。最大带宽填入 1024kbit/sec，表示每个 IP 最多只能使用到 1M/sec 的带宽。带宽共享方式选择"此范围每一 IP 地址最大及最小可用带宽"，如此每一个 IP 最小一定有 2kbit/sec 的保证。

勾选激活，最后点击“新增”即可将此规则加入。

第二条规则接口位置勾选广域网 1、2，服务端选择“ FTP[TCP /21~21”，在 IP 地址填入 0.0.0.0 到 0(表示所有的地址)，目的选择下载。最小带宽填入 2 kbit/sec，表示 FTP 下载保证有 2kbit/sec 的带宽。最大带宽填入 512kbit/sec，表示 FTP 下载最多只能使用到 512kbit/sec 的带宽。带宽共享方式选择“此 IP 地址共享此设置带宽”，如此不论内网有多少人使用 FTP，所有 FTP 下载的带宽总和最多只能使用 50kbit/sec。勾选激活，最后点击“新增”即可将此规则加入。

请注意！QoS 带宽管理的执行顺序为由列表最下面那一条往上做执行动作，所以要将先执行的规则往最下面移。以这个范例来说，先执行 FTP 的共享带宽，在执行每个 IP 的保证以及最大可用带宽。因此若是内网有人使用 FTP 下载，就会先受到第一条规则的限制，最大只能用到 512kbit/sec。若是将规则反过来，将上述的第一条规则移到最下方来先执行，则每个 IP 最大可用到 1M 的带宽，此时用 FTP 下载也就可以用到 1M 的带宽，那么后执行的 FTP 带宽限制在 512kbit 就不会执行，也没有意义了！

QoS带宽管理

控制类型：◉ 带宽控制 ○ 优先级

接口位置：☑ 广域网1 ☑ 广域网2

服务端口：FTP [TCP/21~21]

服务端口新增或删除表

IP地址：0 . 0 . 0 . 0 到 0

目的：下载

保证带宽：2 Kbit/sec 最大可用带宽：512 Kbit/sec

带宽分配方式：○ 此范围每一IP地址独享此设定带宽. ◉ 此范围所有IP地址共享此设定带宽.

激活：☑

上移 更新特殊应用软件 下移

Not Check Port[TCP&UDP/0~0]->192.168.1.100~150(下载)=>2~1024Kbit/sec->WAN1, 2
FTP [TCP/21~21]->0.0.0.0~0(下载)=>2~512Kbit/sec->WAN1, 2

删除选中的项目 新增

优先级- 依优先级做管理：

优先级顾名思义就是可以将您选定想要的服务做先后顺序的调配，也就是可以直接选择服务端口将其优先级做一分配。

QoS 安全路由器会将带宽做 60%(最高)、10%(最低)的带宽分配，也就是若您将 80 端口选择为高级，那么路由器只要遇到 80 端口的数据包就会给予 60%的带宽出去，若您将 FTP 端口 21 设置为低级，那当有人使用 Port 21 时，路由器只会给它 10%的带宽使用，其余未做分配的服务端就使用 30%带宽。

QoS带宽管理

控制类型： ○ 带宽控制 ⦿ 优先级

接口位置： ☐ 广域网1 ☐ 广域网2

服务端口： DNS [UDP/53~53]

服务端口新增或删除表

目的： 上传

优先级： 高级

激活： ☐

增加到对应列表

删除选中的项目

接口位置：	勾选此条选择优先权的设置要控制在哪条 WAN 执行。
服务端口：	在此选择此条优先权所要设置的服务端口为哪个，要针对譬如 FTP 上传或下载，则选择 FTP Port21~21，可参考下拉菜单服务号码默认列表。

目的：	上传： 指针对此服务端口的上传做优先权控制。 下载： 指针对此服务端口的下载做优先权控制。 虚拟服务器上传(Server in LAN，上传)：若您有架设对外的 Server 网站在路由器内部，则此选项为控制外部访问此 Server 的带宽控制。 虚拟服务器下载(Server in LAN，下载)：若您有架设网站在路由器内网，则此选项为控制外部对此服务器上传数据时的带宽控制，例如网吧很多都有架设游戏服务器，若外部要来做此游戏服务器做数据升级时，可以用此控制做带宽管理，才不会影响内部使用者上网打游戏。
优先级：	**高级：** 此为保证 60%的带宽给此服务端口使用。 **低级：** 此为只给 10%的带宽给此服务端口使用。
激活：	启用此规则。
增加到对应列表：	增加此条规则到列表。
删除所选中的项目：	删除所选择在服务列表里的项目内容。
显示开启表：	可以显示出您所有在优先权设置的规则，并可直接点击“编辑”做修改。
确定：	点击此按钮“确认”即会存储刚才所变动的修改设置内容参数。
取消：	点击此按钮“取消”即会清除刚才所变动的修改设置内容参数，此操作必须于确认存储动作之前才会有效。

Smart QoS

无需网管进行烦琐配置的智能型带宽管理 Smart QoS 功能，自动压抑占用带宽用户，来解决内网 QoS 管理的问题，简化网管的管理工作。

☑ 激活动态智能QoS

当任一广域网带宽使用率到达 60 %时，激活智能QoS(此值为0表示永久激活)

☑ 内网IP在所有广域网最大容忍上传带宽 : 500 Kbit/sec

☑ 内网IP在所有广域网最大容忍下载带宽 : 1000 Kbit/sec

当任一IP使用超过上述设定上传或下载带宽时，此IP则使用下列指定频宽

上传带宽 (广域网1 : 300 Kbit/sec 广域网2 : 300 Kbit/sec 广域网3 : 300 Kbit/sec 广域网4 : 300 Kbit/sec)

下载带宽 (广域网1 : 300 Kbit/sec 广域网2 : 300 Kbit/sec 广域网3 : 300 Kbit/sec 广域网4 : 300 Kbit/sec)

☐ 激活二次惩罚

显示惩罚列表 高级设定

管制时间为 所有时间 0 : 0 到 0 : 0 (时间格式:24小时制)

☐ 每天 ☐ 周日 ☐ 周一 ☐ 周二 ☐ 周三 ☐ 周四 ☐ 周五 ☐ 周六

激活动态智能 QoS: 勾选激活动态智能 QoS。

当任一广域网带宽使用率到达___%时，激活智能 QoS 当带宽使用率到达实际带宽的一个%比时，将激活智能 QoS 功能，您可输入需要的数值，系统预设是 60%。

内网 IP 在所有广域网最大容忍上传带宽： 当带宽使用率超过设定的启动百分比时，系统自动检查单一 PC IP 的上传下载使用带宽，若超过设定的值，将给予惩罚，请填入内网 IP 上传最大容许使用带宽。

由于 Smart QoS 进行带宽检查时，可能会消耗影响部分系统效能，所以假设不太需要管制上传带宽，您可以取消勾选此项目表示不检查上传带宽的使用状态。

内网 IP 在所有广域网最大容忍下载带宽 ：	当带宽使用率超过设定的启动百分比时，系统自动检查单一 PC IP 的上传下载使用带宽，若超过设定的值，将给予惩罚，请填入内网 IP 下载最大容许使用带宽。 由于 Smart QoS 进行带宽检查时，可能会消耗影响部分系统效能，所以假设不太需要管制下载带宽，您可以取消勾选此项目表示不检查下载带宽的使用状态。
当任一 IP 使用超过上述设定上传或下载带宽时，此 IP 则使用下列指定带宽：	当任一 IP 使用超过上述设定上传或下载带宽时，就实行惩罚措施，并以各个广域网络的上传 / 下载分别设定，惩罚后允许使用的带宽是多少
激活二次性惩罚：	点选勾选"激活二次性惩罚："后，VPN 防火墙内部设置好二次惩罚条件，当内部网络上网用户上网过程中的上传与下载达到内部条件将执行二次惩罚。
显示处罚列表：	点选后，在弹出的对话框中将会显示处罚中的 IP，上行限制中，下载限制中以及二次惩罚信息。
管制时间：	选择"所有时间"，此 QoS 设定在所有时间都有效果，如果选择"从___:___到___:___"填入时间段（24 小时记时制，例如 19：00 到 24：00）， 以及勾选"每天/周日/周一/周二/周三/周四/周五/周六"的某一天或者几天，其 QoS 设定在所勾选设定的特定时间段内有效。

8.2 会话数管理

会话数管理可以控制内网的计算机最多能同时建立的会话数。这个功能对网管人员在控制内网使用 P2P 软件如 BT、迅雷、emule 等会造成大量发出会话数的软件提供了非常有效的管理。设置恰当的容许会话数可以有效控制 P2P 软件时所能产生的会话数，相对也使带宽使用量达到一定的限制。

另外，若计算机中了类似冲击波的病毒而产生大量对外发会话请求时，也可以达到抑制作用。

会话数管制设定

联机数设置

○ 关闭	
○ 每一内网 IP 最大对外联机数不可超过 300 联机状态 (session)	
◉ 每一内网 IP 最大对外联机数不可超过 TCP 1500 , UDP 400 联机状态 (session)	
○ 当单一个 IP 联机数到达 200 联机状态 (session)	○ 阻挡此 IP 建立新连线达 5 分钟
	○ 封锁此 IP 所有连线达 5 分钟

关闭： 不使用此会话数管控功能。

每一内网 IP 最大对外联机数不可超过___联机状态 (Session)

此选项为限制每一台内网的计算机最大可建立的对外会话数，当用户计算机使用会话数到达此限制值时，要建立新的会话必须等到之前的会话结束后才能再建立。

例如，当用户使用 BT 或 P2P 等下载且会话数超过此设定值后，当用户又要再开其它服务时会无法使用，除非将使用中的 BT 或 P2P 软件关闭。

每一内网 IP 最大对外联机数不可超过 TCP__UDP__： 除了以会话的总数量做限制之外，你也可选择针对 TCP/UDP 通讯协议类型，个别设定限制值，例如限制单一 TCP 会话数不可超过 150，UDP 会话数不可超过 50。

若有 IP 对外会话数到达__时：	**在___分钟内阻止此 IP 建立新会话：**此选项为当客户端计算机使用会话数到达您的设定数值时，此用户在 5 分钟之内将不能再增加新会话，就算旧会话已经结束，也必须等到设定时间过后才能再建立新的会话。
	在___分钟内封锁此 IP 所有会话：此选项为当客户端计算机使用的会话数到达您的设定数值时，此用户正在使用的所有会话都将被清除，且在 5 分钟之内将不能建立任何会话 (不能上网)，必须等到设定时间过后才能再建立新的会话。

时间排程设定

时间管制设定

管制时间为 所有时间	00 : 00 到 23 : 59 (时间表示:24小时制)
☑ 每天	☐ 周日 ☐ 周一 ☐ 周二 ☐ 周三 ☐ 周四 ☐ 周五 ☐ 周六

选择 “所有时间”，此会话数管制设定在所有时间都有效果，如果选择“从___:___到___:___”填入时间段（24 小时记时制，例如 19：00 到 24：00）， 以及勾选“每天/周日/周一/周二/周三/周四/周五/周六”的某一天或者几天，其设定在所勾选设定的特定时间段内有效。

不受限制的通讯端口或 IP 地址

当有的用户以及 IP（比如公司管理层等），或者是特定需要不受限制的服务通讯端口（公司财务数据的传输，邮件的传输等），管理人员可以设定这些服务通讯端口或者 IP 不受会话管制。

不受限制的服务端口或IP地址

服务端口： 所有端口 [TCP&UDP/1~65535]

服务端口新增或删除表

IP地址 : 192 . 168 . 8 . 0 到 0

激活： ☐

最大会话数限制： ◉ 完全不限制

○ 不可超过 300

增加到对应列表

ICMP [ICMP/0~0]->(192.168.8.0~192.168.8.0)

删除选中的项目

通讯端口： 选择不受限制的通讯端口。

IP 地址： 输入不受限制的单一 IP、IP 地址范围，或者选择不受限制的 IP 群组。

激活： 激活此规则。

最大会话数限制： **完全不限制**：表示所设定的 IP/通讯端口会话完全不受到会话数控管的限制。

不可超过___：表示所设定的 IP/通讯端口会话虽然不受到上方会话数控管的全域限制，但是仍要有一个上限值以避免占用过多频宽。

※请注意！

因为平时 ICMP 类型的通讯协议常常会拿来做为网络侦测的工具，所以系统出厂默认值会将 ICMP 加入到不受限制的清单当中，您可以依据您实际的需求再做调整或删除。

加入到对应列表： 将添加的规则增加到列表中。

删除点选的项目： 选择列表中的规则，删除选中的规则。

8.3 硬件加速服务(未来支持)

本系列路由器產品，除了原本就具有极高的处理效能外，也提供了带宽控管、流量优化相关的「硬件加速」功能，此功能的主要目的在于直接使用硬件来处理、加速不同带宽管理相关的功能，优化流量的分配使用，完全不会消耗到 CPU 与系统整体的资源，使路由器的整体处理速度更快，更能承受大量的联机数量与计算机数量，提供绝佳且稳定的网络使用环境。

将网络游戏或是视频软件所使用的服务端口，做流量的最高优先保证，这可以路由器在流量满载的状况下，优先处理这些最高优先权的游戏或视频流量，使游戏与视频软件即使是在流量满载的状况下仍然使用顺畅不断线。

游戏端口加速

MAC 地址设定：关闭
IP 地址：关闭
通讯协定：TCP
服务端口：
激活：
增加到对应列表

TCP->目的服务端口[80]->激活
UDP->目的服务端口[53]->激活
TCP->目的服务端口[1863]->激活
TCP->目的服务端口[5050]->激活
TCP->目的服务端口[443]->激活

删除所选择对应项目

MAC 地址： 下拉式选单项目表示如下

【1】来源 MAC 地址：流量条件需符合所设定来源 MAC 地址内容，保障优先流量硬件加速功能才会生效。

【2】目的 MAC 地址：流量条件需符合所设定来目的 MAC 地址内容，保障优先流量硬件加速功能才会生效。

【3】无或不需检查：流量条件不需要符合、也不检查任何 MAC 地址内容。

IP 地址： 下拉式选单项目表示如下

【1】来源 IP 地址：流量条件需符合所设定来源 IP 地址内容，保障优先流量硬件加速

功能才会生效。
【2】目的 IP 地址：流量条件需符合所设定目的 IP 地址内容，保障优先流量硬件加速功能才会生效。
【3】无或不需检查：流量条件不需要符合、也不检查任何 IP 地址内容。

通讯协议： 需优先保障、加速的游戏、视频或是其它网络应用的服务端口协议。
可选择 TCP 或 UDP 其中一种协议。

服务端口： 输入需优先保障、加速的游戏、视频或是其它网络应用的服务端口号，范围为 1~65535。

激活： 勾选表示激活此条规则，取消勾选表示不激活此条规则

增加到对应列表： 将添加的规则增加到列表中。

删除所选服务： 选择列表中的规则，删除选中的规则。

九、防火墙设置

本章节介绍防火墙设置的选项，以及网络存取控制的设置，保证网络的安全性。

9.1 基本设置

从防火墙功能的一般设置选项当中，您可以控制开启或是关闭这些选项功能。出厂默认值是将防火墙开启，并关闭不必要的响应。

防火墙：	◉ 激活 ○ 关闭
SPI数据包检测：	◉ 激活 ○ 关闭
防止DoS攻击功能：	◉ 激活 ○ 关闭 高级设定
阻止广域网回应功能：	○ 激活 ◉ 关闭
远程管理功能：	◉ 激活 ○ 关闭 端口：80
允许Multicast組播穿透：	○ 激活 ◉ 关闭
防止ARP病毒攻击：	○ 激活 ◉ 关闭 每秒主动发送 20 笔ARP封包

禁止特殊应用

阻挡：	☐ Java
	☐ Cookies
	☐ ActiveX
	☐ Access to HTTP Proxy Servers

☐ 不受限制的信任域名

阻挡特定服务

关闭
☐ MSN
☐ QQ－腾讯 不受限制的 QQ 号码
☐ 雅虎即时通
☐ PPS 网络电视
☐ PPLIVE

☐ 内网不受限制的 IP 位址

Block File Type

关闭
☐ exe
☐ flash
☐ gif
☐ jpeg
☐ mp3
☐ pdf
☐ png
☐ rar
☐ zip

☐ **内网不受限制的 IP 位址**

防火墙功能： 此为选择开启或关闭防火墙功能。默认激活。

SPI 数据包检测: 此为数据包主动侦测检验技术，防火墙主要运行在网络层，但是通过执行对每个连结的动态检验，也拥有应用程序的警示功能。同时，数据包检验型防火墙可以拒绝非标准的通讯协议所使用的连结。默认激活。

防止 DoS 攻击功能: 此为保护 DoS 攻击，如 SYN Flooding， Smurf， LAND， Ping of Death，IP Spoofing 等。默认激活。

阻止广域网响应功能: 若是选择激活的话，则 QoS 安全路由器会关闭对外的 ICMP 与不正常联机的数据包响应，所以若是您从外部去 ping 此台路由器的 WAN IP 是无法 ping 通的，默认值为开启拒绝对外响应的功能。

远程管理功能: 远程管理功能，若您要通过远程网络，直接联机进 QoS 安全路由器的设置窗口，必需将此功能开启，并于远程于浏览器网址填路由器的外部合法 IP 地址(WAN IP)，并加上默认可修改的控制端口(默认为 80，可更改)。

允许 Multicast 组播穿透： 网络上有许多影音串流媒体，使用广播方式可以让客户端接收此类数据包讯息格式。默认为关闭

防止 ARP 病毒攻击： 此功能为防止内网遭受 ARP 欺骗攻击而造成计算机无法上网，此 ARP 病毒欺骗大多在网吧环境发生，会让所有上网计算机一瞬间掉线或部份计算机无法上网。开启此功能可以避免此种病毒攻击。

禁止特殊应用： QoS 安全路由器支持封锁下列几种的方式连结：Java，Cookies，Active X，HTTP 代理服务器存取。

不受限制的信任域名: 若启动这项功能，使用者可以将信任的网站或者 IP 地址加入可信任的网域中，则 QoS 安全路由器就不会去阻挡可信任网域的网页中所带有的 Java/ActiveX/Cookies 等项目。

确定: 点击此按钮“确定”即会存储刚才所变动的修改设置内容参数。

取消: 点击此按钮“取消”即会清除刚才所变动的修改设置内容参数，此操作必须于“确定”存储动作之前才会有效。

防止 **DoS** 攻擊功能 高级设定

数据包类型	广域网阈值设定			局域网阈值设定		
☑ TCP_SYN_Flooding	所有数据包阈值	15000	Packets/sec	所有数据包阈值	15000	Packets/sec
				单一目的IP的数据包门阈值	0	Packets/sec
	单一IP的数据包阈值	2000	Packets/sec	单一来源IP的数据包门阈值	2000	Packets/sec
	达到阈值便阻挡该IP	5	分钟	达到阈值便阻挡该IP	5	分钟
☑ UDP_Flooding	所有数据包阈值	15000	Packets/sec	所有数据包阈值	15000	Packets/sec
				单一目的IP的数据包门阈值	0	Packets/sec
	单一IP的数据包阈值	2000	Packets/sec	单一来源IP的数据包门阈值	2000	Packets/sec
	达到阈值便阻挡该IP	5	分钟	达到阈值便阻挡该IP	5	分钟
☑ ICMP_Flooding	所有数据包阈值	200	Packets/sec	所有数据包阈值	200	Packets/sec
				单一目的IP的数据包门阈值	0	Packets/sec
	单一IP的数据包阈值	50	Packets/sec	单一来源IP的数据包门阈值	50	Packets/sec
	达到阈值便阻挡该IP	5	分钟	达到阈值便阻挡该IP	5	分钟
☐ 不受限制的来源IP地址	1. IP地址	_ . _ . _ . _ 到 _				
	2. IP地址	_ . _ . _ . _ 到 _				
☐ 不受限制的目的IP地址	1. _ . _ . _ . _					
	2. _ . _ . _ . _					
	3. _ . _ . _ . _					
	4. _ . _ . _ . _					
	5. _ . _ . _ . _					

数据包类型: QoS 安全路由器提供三种数据数据包传输类型，包括 TCP-SYN-Flood、UDP-Flood 以及 ICMP-Flood。

广域网限定值设置： 防止来自外部网络的攻击。设置“所有数据包限定值”（即外部攻击的所有数据包数据），当其达到一个最大值（默认 15000pakets/Sec），QoS 安全路由器将只允许通过所设置最大值的数据包数。

当单一 IP 的数据包限定值（外部单一一个 IP 地址攻击的数据包数据）达到一个最大值(默认 2000pakets/Sec）就会阻挡此 IP 上网 5 分钟（默认是 5 分钟），禁止其访问服务器，限制其流量和连接数，从而有效保证网络的安全。这里您可以根据需要调整你的限定值以及阻挡时间来达到对外网攻击的有效防护，建议其限定值从大到小来调节，避免限定值过小影响正常网络的运行。

局域网限定值设置： 防止来自内部网络的攻击。同样，当所有数据包限定值（即外部攻击的所有数据包数据）达到一个最大值（默认 15000pakets/Sec），QoS 安全路由器将只允许通过所设置最大值的数据包数。

当单一数据包阀值（内部单一一个 IP 地址攻击的数据包数据）达到一个最大值（默认 2000pakets/Sec），就会阻挡此 IP 上网 5 分钟（默认是 5 分钟），禁止其访问服务器，限制其流量和连接数，从而有效保证网络的安全。您可以根据需要调整你的阀值以及阻挡时间来达到对内网攻击的有效防护，建议其阀值从大到小来调节，避免阀值过小影响正常网络的运行。

不受限制的来源 IP 地址： 输入不要被 DoS 防御设置限定值所限制的区域网来源 IP 地址或是范围

不受限制的目的 IP 地址： 输入不要被 DoS 防御设置限定值所限制的目的 IP 地址

(从区域网发出的数据包)

显示被阻挡的 IP：



显示被 DoS 防御功能所阻挡的 IP 地址，以及该 IP 地址还剩余多少时间解除阻挡

阻挡特定服务（一指键）

Qno 防火牆 / 路由器提供一指键封锁特定的服务功能，可以通过设置将特殊服务 MSN、Skype、QQ、这些服务挡住，以方便用户的管理。

阻挡特定服务

关闭

- [x] MSN
- [x] QQ – 腾讯　不受限制的 QQ 号码
- [ ] 雅虎即时通
- [ ] PPS 网络电视
- [ ] PPLIVE

- [x] 内网不受限制的 IP 位址

内网不受限制的 IP 位址

特定服务: MSN

不受限制的 IP 位址 : . . . 到

增加到对应列表

删除所选择的项目

勾选表示会封锁用户对于该应用服务的使用，若是在封锁状态下需开放部分能使用的用户，就必须勾选「内网不受限制的 IP 地址」，并且在下方针对封锁的服务，增加不受限制的 IP 地址清单。

内网不受限制的 IP 地址：　针对以上所封锁的服务，开放内网不受限制的使用者 IP / IP 范围。

特定服务：　选择某个封锁的服务应用，进行不受限制的内网 IP 设定。

不受限制的 IP 地址：　针对上方所选的已封锁的应用服务，设定那些 IP 可以开放使用不受限制。

另外，若激活一指键 QQ，也可以针对某些 QQ 号码能够不受封锁做设置，按下"不受限制的 QQ 号码"，跳出以下窗口即可将不受封锁限制的 QQ 号码输入，增加到下方清单以内：



用户名： 输入能识别此 QQ 号码的信息，例如 Qno Sales。

不受限制的 QQ 号码： 输入不受限制的 QQ 号码。

增加到对应列表： 将添加的规则增加到列表中。

删除选中的项目： 选择列表中的规则，删除选中的规则。

Block File Type：封锁一些常用的文件格式传输，例如 **exe** 文件、**zip** 压缩档案等。

Block File Type

关闭
☑ exe
☑ flash
☑ gif
☑ jpeg
☑ mp3
☑ pdf
☑ png
☑ rar
☑ zip

☑ 内网不受限制的IP位址

内网不受限制的IP位址

特定服务: exe

不受限制的IP 位址: . . . 到

增加到对应列表

删除所选择的项目

勾选表示会封锁用户下载/开启该类型的文件，若是在封锁状态下需开放部分能使用的用户，就必须勾选「内网不受限制的 IP 地址」，并且在下方针对封锁的档案类型，增加不受限制的 IP 地址清单。

9.2 访问规则设置

QoS 安全路由器设计有简而易懂的网络存取规则条例工具，管理者可以用来对不同的使用者设置不同的存取规则条件，来管理使用者对网络的存取权限。存取规则可以依据不同的条件来过滤，例如可以设置数据包要管制的进出方向是从内部到外部还是从外部到内部，或是设置以使 IP 地址、目地端 IP 地址、IP 通讯协议状态等条件来做管制，管理者可以依照实际的需求调性设置。

9.2.1 默认管制规则

管理者定订的网络存取规则条例，可以选择关闭或是允许来调整使用者对网络的存取。以下就针对 QoS 安全路由器的网络存取规则条例做一说明：

QoS 安全路由器默认的网络存取规则条例：

*从 LAN 端到 WAN 端的所有数据包可以通过-All traffic from the LAN to the WAN is allowed

*从 WAN 端到 LAN 端的所有数据包不可以通过-All traffic from the WAN to the LAN is denied

*从 LAN 端到 DMZ 端的所有数据包不可以通过-All traffic from the LAN to the DMZ is denied

*从 DMZ 端到 LAN 端的所有数据包不可以通过-All traffic from the DMZ to the LAN is denied

*从 WAN 端到 DMZ 端的所有数据包不可以通过-All traffic from the WAN to the DMZ is denied

*从 DMZ 端到 WAN 端的所有数据包不可以通过-All traffic from the DMZ to the WAN is denied

管理者可以自定存取规则并且超越 QoS 安全路由器的默认存取条件规则，但是以下的四种额外服务项目为永远开启，不受其它自定规则所影响：

* HTTP 的服务从 LAN 端到 QoS 安全路由器 默认为开启的 (为了管理 QoS 安全路由器使用)。

* DHCP 的服务从 LAN 端到 QoS 安全路由器 默认为开启的 (为了从 QoS 安全路由器自动取得 IP 地址使用)。

* DNS 的服务从 LAN 端到 QoS 安全路由器 默认为开启的 (为了解析 DNS 服务使用)。

* Ping 的服务从 LAN 端到 QoS 安全路由器 默认为开启的 (为了连通测试 QoS 安全路由器使用)。

跳到 1 / 2 页　　每页显示 5 笔　　下一页>>

优先级	激活	管制动作	服务端口	接口位置	来源IP地址	目的IP地址	管制时间	日	编辑	删除
	☑	允许	所有端口 [*]	局域网	任何的	任何的	所有时间			
	☑	关闭	所有端口 [*]	广域网1	任何的	任何的	所有时间			
	☑	关闭	所有端口 [*]	广域网2	任何的	任何的	所有时间			
	☑	关闭	所有端口 [*]	广域网3	任何的	任何的	所有时间			
	☑	关闭	所有端口 [*]	广域网4	任何的	任何的	所有时间			

添加新规则　恢复出厂默认值

除了默认规则以外， 所有的网络存取规则都会显示于此规则列表中，您可以自己选择高低优先权于每一个网络存取规则项目中。QoS 安全路由器在做规则确认时是依照优先权 1-2-3...。依序做规则判断，所以优先权是让您在做存取规则的设置规划中必须要考虑的，以避免您想开启或关闭的功能失效。

编辑： 可以设置网络存取规则项目。

垃圾桶图像： 可以删除网络存取规则项目。

添加新规则： 新增新的网络存取规则按钮可以新增一项新的存取规则。

恢复出厂默认值： 可以恢复到出厂原有默认存取规则项目并删除所有的自定规则内容。

9.2.2 增加新的管制规则

访问规则设置

管制动作：	允许
服务端口：	所有端口 [TCP&UDP/1~65535] 服务端口新增或删除表
日志：	关闭
接口位置：	局域网
来源IP地址：	单独 . . .
目的IP地址：	单独 . . .

生效时间

管制时间为 所有时间	: 到 : (时间格式:24小时制)
每天	周日 周一 周二 周三 周四 周五 周六

返回 确定 取消

管制动作: 允许： 允许符合此管制条例行为的数据包通过。

关闭： 不允许符合此管制条例行为的数据包通过。

服务端口: 从下拉式选单中选择您所要允许或不允许的服务端口服务项目内容。

服务端口新增或删除表: 若是您想要管制的服务端口服务内容没有存在于默认列表内的话，您可以点击右方的服务端新增或删除表来新增一个服务内容。于弹出窗口中输入一个服务名称以及通讯协议与端口，点击"新增"按钮即可新增一个管制服务项目内容。

日志: 允许: 依据此规则发生的相关事件将在日志中记录。

关闭: 依据此规则发生的相关事件不会日志中记录。

接口位置: 选择您所要允许或不允许的来源数据包接口(例如是从 LAN， WAN1，WAN2 还是任何的)，可以从下拉式选单中选择。

来源 IP 地址: 选择来源数据包的 IP 范围(如任何的，单独或者范围)，若是选择单独是范围的话，请输入此单一或是一区段范围的 IP 地址。

您也可以选择 IP 群组的方式来指定来源 IP。关于 IP 群组的设置，请参考（"7.6 IP 群组管理"说明）。

目的 IP 地址: 选择目的端数据包的 IP 范围(如任何的，单独或者范围)，若是选择单独是范围的话，请输入此单一或是一区段范围的 IP 地址。

生效时间设置: 您可以将此条规则依照您所需要的执行时间来做控管。例如您可以设置此

	规则每天上午 8：00 开始执行下午 17：00 结束，或 24 小时都执行管制。
应用此存取规则:	选择“所有时间”表示都 24 小时都执行此规则(默认)，或是可以选择从几点到几点，以及设置是每天还是某几天做管制。
…到…：	…到…：此管制规则有时间限制，设置方式为 24 小时制，如 08：00 到 18：00 (早上 8 点到下午 6 点)。
管制天数:	勾选“每天”是表示每一天的这段时间都受控管，若是只针对一星期特定星期几，可以直接选择星期。
确定:	点击此按钮“确认”即会存储刚才所变动的修改设置内容参数。
取消:	点击此按钮“取消”即会清除刚才所变动的修改设置内容参数，此操作必须于确认存储动作之前才会有效。

<u>范例 1：若要将病毒端口 TCP 135-139 封锁要如何设置?</u>

首先在服务端口新增部份加入 TCP 135-139 端口(请参考如何新增服务端口的章节)，然后进行以下的设置：

管制动作：禁止

服务端口：TCP135-139

来源接口：任何的(此意思为封锁由内网往外网以及从外网攻击内网的任何此端口)

来源 IP 地址：任何的(此意思为封锁由内网往外网以及从外网攻击内网的任何此端口)

目的 IP 地址：任何的(此意思为封锁由内网往外网以及从外网攻击内网的任何此端口)

访问规则设置

管制动作：	禁止
服务端口：	TCP[TCP/135~139] 服务端口新增或删除表
日志：	关闭
接口位置：	任何的
来源IP地址：	任何的
目的IP地址：	任何的

范例 2：若要禁止内网 IP 段 192.168.1.200 到 192.168.1.230 禁止访问 80 端口要如何设置?

管制动作：:禁止

服务端口：TCP 80

来源界面：局域网(此意思为封锁由内网往外网的 80 端口)

来源 IP 地址：范围 192.168.1.200 到 192.168.1.230

目的 IP 地址：任何的(此意思为封锁由 192.168.1.200 到 192.168.1.230 内网往外网任何 80 端口)

访问规则设置

管制动作：	禁止	
服务端口：	HTTP[TCP/80~80]	服务端口新增或删除表
日志：	关闭	
接口位置：	局域网	
来源IP地址：	范围	192 . 168 . 1 . 200 到 192 . 168 . 1 . 230
目的IP地址：	任何的	

9.3 网站内容过滤

网站内容过滤可支持两种模式的网页管制，一为封锁禁止访问的域名，另一个为允许访问的域名，此两种模式只能使用一种。

设定允许访问的域名
设定禁止访问的域名

9.3.1 设定 / 封锁禁止访问的域名

此功能需将完整的域名如 www.sex.com 填入，即可封锁此网站。

设定允许访问的域名
设定禁止访问的域名

禁止访问的域名

激活

域名 :

不受限制的IP地址 : 0 . 0 . 0 . 0 到 0

增加到对应列表

chinatrust->管制所有IP位址
consumer.chinatrust.com.tw->管制所有IP位址

删除选中的项目

设定禁止访问/连接的域名: 设定那些是受管制禁止访问的域名。

激活管制/禁止访问的域名功能: 开启网页管制内容项目。

域名: 填写欲管制的网址，如 www.playboy.com。

不受限制的 **IP** 地址： **不受限制 IP 地址/IP 群组：**

设定那些 IP/IP 群组可以不受限制访问上方所设定的网页。

其它不在不受限制的 IP 范围内，就会受到限制并且无法访问上方所设定的网页。

管制所有 IP 地址：
表示所有 IP 地址皆会受到管制并且无法访问上方所设定的网页。

加入到对应列表: 点选"增加到对应表"按钮新增此一欲管制的网址。

删除点选的项目: 可以使用鼠标点选一个或多个管制的网址，然后点选即可删除。

网页内容过滤(关键词)：

○ 设定允许访问的域名
◉ 设定禁止访问的域名

禁止访问的域名

☐ 激活

网页内容过滤(关键字)

☑ 激活

关键字：[ ] (仅支持英文关键字)

不受限制的IP地址 ▾ : 0 . 0 . 0 . 0 到 0

增加到对应列表

chinatrust->管制所有IP位址

删除选中的项目

激活网页内容过滤（关键词）功能： 当此项功能激活后，当输入网站地址有存在 "sex"关键词时，则会将所有有"sex"的网页封锁。

关键词（仅支持英文关键词）： 输入关键词。(目前只支持英文关键词，不支持中文或其它语言)

不受限制的 IP 地址： **不受限制 IP 地址/IP 群组：**

	设定那些 IP/IP 群组可以不受限制访问含有上方设定关键词的网页。其它不在不受限制的 IP 范围内，就会受到限制并且无法访问含有上方设定关键词的网页。 **管制所有 IP 地址：** 表示所有 IP 地址皆会受到管制并且无法访问含有上方设定关键词的网页。
加入到对应列表:	增加此新增的服务项目内容到服务表列内。
删除选中的的项目:	选择删除服务项目内容从服务表列内。

生效时间设定：

当选择为“所有时间”时，表示此条规则每天并且 24 小时皆会生效，随时进行管制检查；选择为“从”时，可以在单一天中设定三个时段，以及选择那几天（或是每天）在此三个时段规则生效并进行管制检查。

生效时间

管制时间为 所有时间	: 到 : (时间格式:24小时制)
	: 到 : (时间格式:24小时制)
	: 到 : (时间格式:24小时制)
☐ 每天	☐ 周日 ☑ 周一 ☑ 周二 ☑ 周三 ☑ 周四 ☑ 周五 ☐ 周六

※请注意！所设定的三个时间区段不能重复！

9.3.2 允许访问的域名

此功能的目的是设定只能去访问的网址，在有些公司或学校中，会只允许员工或学生只能去哪些网站，就可以用此功能来达成。

◉ 设定允许访问的域名
○ 设定禁止访问的域名

允许访问的域名

☑ 激活

域名：

增加到对应列表

www.baidu.com
www.google.com
tw.yahoo.com

删除选中的项目

生效时间

管制时间为 所有时间	: 到 : (时间格式:24小时制)
	: 到 : (时间格式:24小时制)
	: 到 : (时间格式:24小时制)
☐ 每天	☐ 周日 ☑ 周一 ☑ 周二 ☑ 周三 ☑ 周四 ☑ 周五 ☐ 周六

不受限制的IP地址

IP地址 : . . . 到

增加到对应列表

删除选中的项目

激活允许访问的域名功能： 选择打勾开启允许网址管制功能，预设为关闭。
激活此功能后，只有加到允许访问网页清单的网站才能够进行访问，其它未加入清单的网站会被封锁无法访问。

域名: 填写欲管制的允许网址，如 www.google.com。

时间排程设定： 当选择为“所有时间”时，表示此条规则每天并且 24 小时皆会生效，随时进行管制检查；选择为“从”时，可以在单一天中设定三个时段，以及选择那几天（或是每天）在此三个时段规则生效并进行管制检查。

※请注意！所设定的三个时间区段不能重复！

時間排程設定

管制時間為 所有時間	: 到 : (24小時制)
	: 到 : (24小時制)
	: 到 : (24小時制)
☐ 每天	☐ Sun ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri ☐ Sat

不受限制的 IP 地址： 不受限制 IP 地址/IP 群组：
设定那些 IP/IP 群组可以不受限制可以访问所有的网站。
其它不在不受限制的 IP 范围内，就会受到限制并且只能访问上方所设定的网页。

十、其它进阶高级功能设置

本章介绍 QoS 安全路由器进阶功能的设置，如果内网需要设置服务器提供 Web/FTP 服务等，可以通过虚拟服务器的连接设置设置完成，同时应部分用户需要提供静态路由以及动态路由协议的设置，一对一 NAT 功能的设置解决实体 IP 与虚拟 IP 对应，以及设置动态域名解析服务满足用户获得运营商的动态公网 IP 情况下需要建设 Web/FTP 服务器等要求。

10.1 DMZ/虚拟服务器

DMZ Host

内部DMZ服务器IP地址 (DMZ Host) : 10 . 10 . 0 . 0

虚拟服务器

服务端口 : 所有端口 [TCP&UDP/1~65535]

服务端口新增或删除表

内部IP地址 : 10 . 10 . 10 .

激活 :

增加到对应列表

删除选中的项目

10.1.1 DMZ 设置

当您将 QoS 安全路由器内部的某台 PC 的虚拟 IP 填入到此 DMZ 选项时， QoS 安全路由器 WAN 端的合法 IP 地址会直接对应给此台 PC 使用，也就是说从 WAN 端进来的数据包，若是不属于内部的任何一台 PC，都会传送到这台 PC 上。

在使用“DMZ 主机”功能后，若您要取消此功能必须于在设置虚拟 IP 地址地方填入“0” 的参数，才会停止此功能使用。

点击此按钮“确认”即会存储刚才所变动的修改设置内容参数。 点击“取消” 即会清除刚才所变动的修改设置内容参数，此操作必须在确认存储动作之前才会有效。

10.1.2 虚拟服务器设置

若是您需在内网需架设服务器（意指对外部的服务主机 WEB、FTP、Mail 等），这个功能可将服务器主机视为一个虚拟位置，利用 Qno 防火墙/路由器的外部合法 IP 地址，经过通讯端口的转换，（如 WWW 为 80 端口），直接存取到内部虚拟 IP 的服务器的服务。

例如在设定窗口中，选项填入服务器位置，如 192.168.1.2 且端口是 80 的话，当外部网络要进来存取这个网页时只要键入：

http：//220.130.188.45 (假设此为 Qno 防火墙 / 路由器的外部合法 IP 地址)

此时，就会通过此公网 IP 地址去转换到 192.168.1.2 的虚拟主机上的 80 端口读取网页了。

其它种类的服务器设定，都如以上设定；只要将所用服务器的通讯端口以及虚拟主机的 IP 地址填入即可！

虚拟服务器

服务端口： 所有端口 [TCP&UDP/1~65535]

服务端口新增或删除表

内部IP地址： 192 . 168 . 8 .

接口位置： ANY

激活：

增加到对应列表

删除选中的项目

服务端口： 在此选择欲开启的虚拟服务器的通讯端口号码预设列表，如 WWW 为 80(80~80)， FTP 为 21~21，可参考服务号码预设列表！

服务端口设定： 若您所需要的通讯端口没有在列表里面，可以利用此功能新增或删除管理通讯端口号列表。

内部 IP 地址： 在此填上虚拟服务器所要相对应的内部虚拟 IP 地址，如 192.168.8.100。

接口位置： 设定内部服务器通讯端口转换所对应的广域网界面是那一个，您可以设定外部用户只能从某一个广域网界面 (某一个合法 IP) 进来存取服务器的服务。

启用： 开启此服务功能。

加入到对应列表： 增加到开启服务项目内容。

新增或删除通讯端口号

若您欲开启的服务埠项目没有在表列中，您可以点击“服务端新增或删除表”新增或删除管理服务埠号列表，如下图所示：

服务端口名称

通讯协定

TCP

服务端口范围

到

All Traffic [TCP&UDP/1~65535]
DNS [UDP/53~53]
FTP [TCP/21~21]
HTTP [TCP/80~80]
HTTP Secondary [TCP/8080~8080]
HTTPS [TCP/443~443]
HTTPS Secondary [TCP/8443~8443]
TFTP [UDP/69~69]
IMAP [TCP/143~143]
NNTP [TCP/119~119]
POP3 [TCP/110~110]
SNMP [UDP/161~161]
SMTP [TCP/25~25]
TELNET [TCP/23~23]
TELNET Secondary [TCP/8023~8023]

增加到对应列表　删除所选择服务服务端口

确定　取消　退出

服务端口名称：	在此自定欲开启的服务埠号名称加入列表中，如 BT 等。
通讯协议：	在此选择欲开启的服务埠号的封包格式为 TCP 或 UDP。
服务埠范围：	将您所需新增加的服务埠范围填入。
增加到对应列表：	增加到开启服务项目内容列表，最多可新增 100 组。
删除选择服务服务端口：	删除所选择的开启服务项目之一笔内容。
确定：	点击此按钮“**确认**”即会储存刚才所变动的修改设定内容参数。
取消：	点击此按钮“**取消**”即会清除刚才所变动的修改设定内容参数，此操作必须于确认储存动作之前才会有效。
退出：	离开此功能设定窗口。

10.2 UPnP 通讯协议

UPnP (Universal Plug and Play) 是微软所制定的一项通讯协议标准，若是您使用的计算机有支持 UpnP 机制的话(如 Windows XP)而且您的计算机 UpnP 功能有开启，您可以将 QoS 安全路由器的 UPnP 功能启动，可以从您的计算机上开启或关闭 UPnP Forwarding 的选项。

UPnP 功能包含有 UPnP Forwarding 的功能，如您要在内网设置虚拟服务器，您可以在前章节介绍的 Forwarding 功能设置，或是在此 UPnP Forwarding 中设置。不过请不要重复输入造成冲突。

UPnP手动映射

服务端口：DNS [UDP/53->53]
服务端口新增或删除表
主机名称 或 IP地址：
激活：
增加到对应列表
删除选中的项目
显示开启表　确定　取消

服务端口：	在此选择欲开启的 UPnP 的服务号码默认列表，如 WWW 为 80(80~80)，FTP 为 21~21，可参考服务号码默认列表！
主机名称或 IP 地址：	在此填上 UPnP 相对应的内部虚拟 IP 地址或名称，如 192.168.1.100。
激活：	开启此服务功能。
服务端口增加或删除表：	新增或删除管理服务端口号列表。
增加到对应列表：	增加到开启服务项目内容。
删除所选中的项目：	删除所选择的开启服务项目之一笔内容。
显示开启表：	显示目前所开启设置的 UpnP Forwarding 列表。
确定：	点击此按钮“确认”即会存储刚才所变动的修改设置内容参数。
取消：	点击此按钮“取消”即会清除刚才所变动的修改设置内容参数，此操作必须于确认存储动作之前才会有效。

10.3 路由通讯协议

此节介绍动态路由协议以及静态路由的设置。

动态路由

工作模式：	⦿ NAT模式 ○ 路由模式
RIP路由协议功能：	○ 激活 ⦿ 关闭
RIP路由协议版本(接收端)：	Both RIP v1 and v2
RIP路由协议版本(传送端)：	RIPv2 - Broadcast

静态路由

目的IP地址：
子网掩码：
网关：
路由节点数：
接口位置：局域网
增加到对应列表
删除选中的项目

10.3.1 动态路由设置

RIP 是路由通讯协议 Routing Information Protocol 的简称，有 RIP I / RIP II 两个版本。对于一般使用的网络中，大多只有一个路由器(或是网关器)，所以大部份的情况是不需要使用这个功能。RIP 的使用时机是您的网络中有数个路由器，此台 QoS 安全路由器是其中之一，此时若是不想手动设置每台路由器的绕径表，可以启动此功能，自动将所有路径更新！

RIP 是一个很非常简单的路由协议，采用距离向量的方式以数据包到达目的地之前需要经过的路由的个数来做传送距离的判断，而不以实际联机的速率来做判断。所以所选的路径是经过最少的路由，但是并不一定反应速度最快的路由及路径。

动态路由

工作模式：	◉ NAT模式 ○ 路由模式
RIP路由协议功能：	◉ 激活 ○ 关闭
RIP路由协议版本(接收端)：	Both RIP v1 and v2
RIP路由协议版本(传送端)：	RIPv2 - Broadcast

选择路由器工作模式： 选择 QoS 安全路由器运作模式为 NAT 模式或是路由模式。

动态路由通讯协议 RIP 功能： 选择按钮“激活”开启使用 RIP 动态路由通讯。

RIP 路由协议版本（接收端）： 可于上下选择按钮选择使用动态路由通讯 None， RIPv1， RIPv2，Both RIPv1 and v2 作为传送动态路由通讯协议格式。

RIP 路由协议版本（传送端） 可于上下选择按钮选择使用动态路由通讯 None， RIPv1，RIPv2-Broadcast， RIPv2-Multicast， 为接收动态路由通讯协议格式。

10.3.2 静态路由设置

静态路由是以手动设置路由表的方式来达成数据包路由。在此 QoS 安全路由器的应用可分为两种方式，一是在内网中连结不同网段或路由器，一是在 Multi-WAN 的环境中让路由器知道去那个目地地址时就要走那条 WAN。例如常常会遇到路由器不同的 WAN 申请不同运营商的线路，为了避免有些服务像是邮件服务器，或游戏服务器是架设在不同一运营商环境而且运营商之间无法彼此互通，此时去邮件服务器或是去游戏服务器就应该走不同的 WAN，而避免绕远路。这个用意跟协议绑定是有相似的做用。

静态路由

目的IP地址 : . . .
子网掩码 : . . .
网关 : . . .
路由节点数 :
接口位置 : 局域网
增加到对应列表
删除选中的项目
显示开启表 确定 取消

目的 IP 地址和子网掩码：	填入目的地的远程网络 IP 节点与子网络节点地址。
默认网关：	从此网络节点到目的远程网络欲绕径的默认网关器地址。
路由节点数：	从此网络节点到目的远程网络所经过 QoS 安全路由器层数，如是在 QoS 安全路由器下的二个 QoS 安全路由器之一，此应填为 2，默认为 1。(最大为 15)。
接口位置：	此网络节点的连接位置，是位于广域端口 WAN 端亦或是局域端口 LAN 端。
增加到对应列表：	增加此路径规则到列表中。
删除所选中的项目：	删除在表中所选择的路径表。
显示开启表：	显示目前最新的路径表。
确定：	点击此按钮“确认”即会存储刚才所变动的修改设置内容参数。
取消：	点击此按钮“取消”即会清除刚才所变动的修改设置内容参数，此操作必须于确认存储动作之前才会有效。

10.4 一对一 NAT 对应

当您的运营商线路为固定制(如 ADSL 固定 IP)时，通常运营商会给您多个合法 IP 地址。QoS 安全路由器提供您可将除了路由器本身 WAN 端口以及光纤盒或 ATU-R(网关) 各使用一个合法 IP 地址后，所剩的合法 IP 地址可以直接对应到路由器内部的计算机使用，也就是这些计算机在内网虽为虚拟 IP，但当做了一对一对应后，这些对应到的计算机去外部访问时都是有自己的合法 IP。

例如，当您公司内部环境需有两台或两台以上的"WEB 服务器"时，由于需要两个或两个以上的合法 IP 地址，所以可以利用此功能达到将外部多个合法 IP 地址直接对应到内部多个虚拟服务服务器 IP 地址使用！

范例： 如您有 5 个合法 IP 地址，分别是 210.11.1.1～6，而 210.11.1.1 已经给 QoS 安全路由器的 WAN1 使用，另外还有其它四个合法 IP 可以分别设置到 One to One NAT 当中，如下所述：

210.11.1.2→ 192.168.1.3

210.11.1.3→ 192.168.1.4

210.11.1.4→ 192.168.1.5

210.11.1.5→ 192.168.1.6

注意！

QoS 安全路由器 WAN IP 地址不能被涵盖在一对一 NAT 的 IP 范围设置中。

☑ 激活一对一NAT 功能

内部起始IP地址：10 . 10 . 10 .
外部起始IP地址： . . .
对应范围的IP数量：
增加到对应列表

删除选中的项目

确定 取消

激活一对一 NAT 功能:	选择是否开启此一对一 NAT 功能 "激活"开启 "禁止"关闭。
内部起始 IP 地址:	虚拟 IP 地址起始 IP 地址。
外部起始 IP 地址:	外部合法 IP 地址起始 IP。
对应范围的 IP 数量:	填入您同时要有多少个外部合法 IP 地址需要对应。
增加到对应列表:	加入此设置到一对一 NAT 列表中。
删除选中的项目:	删除所选择的一对一 NAT 规则。
确定:	点击此按钮"确认"即会存储刚才所变动的修改设置内容参数。
取消:	点击此按钮"取消"即会清除刚才所变动的修改设置内容参数，此操作必须于"确定"存储动作之前才会有效。

注意！

一对一的 NAT 模式将会改变防火墙运作的方式，您若设置了此功能，LAN 端所对应有 公网 IP 的服务服务器或计算机将会曝露在互联网上。若要阻绝网络的使用者主动联机到一对一 NAT 的服务服务器或计算机，请到防火墙的存取规则中设置适当的拒绝存取规则条件。

Multiple To One 多对一对应

当您需要设定某部分内网 IP 地址 / 范围，固定转 NAT 某个 WAN IP 出去，用来注册特别的服务或是网络架构，就可以透过多对一 NAT 对应进行设定。

激活多对一NAT功能 ☑

多对一NAT功能

内部IP地址范围: 到

对应的广域网IP地址:

接口位置 广域网1

增加到对应列表

删除所选择对应列表

激活多对一 NAT 功能: 选择是否开启此多对一 NAT 功能。

内部 IP 地址范围: 内网虚拟 IP 地址范围。

对应的广域网 IP 地址: 设定固定对应的广域网 (WAN) IP 地址，需搭配下方所选择的广域网线路，若该 IP 地址不在该广域网界面包含的范围之内，设定是无效的。

接口位置： 选择广域网 IP 所对应的界面，，若上方对应 WAN IP 地址不在该广域网界面包含的范围之内，设定是无效的。

增加到对应列表: 加入此设定到多对一 NAT 列表中。

删除所选对应列表: 删除所选择的多对一 NAT 规则。

确定: 点击此按钮"确认"即会存储刚才所变动的修改设定内容参数。

取消: 点击此按钮"取消"即会清除刚才所变动的修改设定内容参数，此操作必须于"确定"存储动作之前才会有效。

10.5 DDNS-动态域名解析

此 QoS 安全路由器的 “DDNS” 功能可以支持 QnoDDNS.org.cn、Dyndns.org、3322.org（支持 DDNS 种类依机种不同而相异）的动态域名解析功能，其目的是为了让使用动态 IP 地址(也就是无法有固定 IP 的环境)来架设虚拟服务器、建立企业使用、及远程监控时查询现在的路由器 IP。如 ADSL PPPoE 计时制或是 Cable Modem 的使用者的 WAN IP 地址都会随运营商端要求而改变，当此时使用者申请了 DDNS 后，如“qno. QnoDDNS.org.cn”，将其设置在 DDNS 设置中，则在远程只要去 Ping QnoDDNS.org.cn 则可以知道现在 QoS 安全路由器的实际 IP。且若是内部有架设网站之类的服务，网络使用者只要在网址打上 qno. QnoDDNS.org.cn 就可以直接进入到您内部架设的 WEB。在设置此功能之前，请向 www.qno.cn/ddns、www.dyndns.org 或是 www.3322.org 提出申请，此服务是完全免费的！

另外，为了解决 DDNS 服务器可能会发生不稳定的情况，现在 QoS 安全路由器每个 WAN 都可同时对此二家 DDNS 做动态 IP 升级。

动态域名服務

接口位置	动态域名	状态	配置
广域网1	Dyndns:--- 3322:--- Dtdns:--- Qnoddns:---	Dyndns 关闭 3322 关闭 Dtdns 关闭 Qnoddns 关闭	编辑
广域网2	Dyndns:--- 3322:--- Dtdns:--- Qnoddns:---	Dyndns 关闭 3322 关闭 Dtdns 关闭 Qnoddns 关闭	编辑

*此为示意图，会因产品线不同，图形会有所差异

选择您要设置的广域网端口，比如“广域网 1”，点击“编辑”进入广域网 1 的 DDNS 设置窗口，对要设置的 WAN 口的 DDNS 方式进行勾选。

接口位置: WAN1

☑ DynDNS.org

用户名:	注册
密码:	(密码不能含有字符串'password')
动态域名:	. .
广域网 IP地址:	0.0.0.0
状态:	DDNS功能关闭或是没有联机

☑ 3322.org

用户名:	注册
密码:	(密码不能含有字符串'password')
动态域名:	. .
广域网 IP地址:	0.0.0.0
状态:	DDNS功能关闭或是没有联机

☐ QnoDDNS.org.cn

返回 确定 取消

接口位置	显示使用者所选取的广域端口
DDNS 动态域名解析服务：	可以选择 QnoDDNS.org.cn 以及 3322.org(可以同时使用)（支持 DDNS 种类依机种不同而相异）
用户名称：	向 DDNS 服务提供者所申请的使用者名称。QnoDDN 使用者名称要填入完整的网址，如：abc.qnoddns.org.cn。
密码：	向 DDNS 服务提供者所申请的密码。
动态域名：	动态网址名称： 向 DDNS 所注册的网址，如 abc.QnoDDNS.org.cn 或者 abc.dyndns.org。
广域网 **IP** 地址：	目前此条 WAN 所取得的运营商之动态合法 IP 地址，当 QoS 安全路由器得到运营商端给的合法 IP 地址后会自动显示于此。
状态：	显示目前 QoS 安全路由器对 DDNS 的更新状态。
确定：	点击此按钮“确认”即会存储刚才所变动的修改设置内容参数。
取消：	点击此按钮“取消”即会清除刚才所变动的修改设置内容参数，此操作必须于确认存储动作之前才会有效。

注册 QnoDDNS 侠诺动态域名

1．请先至 Qno 侠诺网站，进行产品注册：http://www.qno.cn

2．依据产品注册使用的电邮以及产品序列号，登入 QnoDDNS 侠诺动态域名服务系统；请确认电邮可以确实收信，以利注册域名后，可收到系统寄出的启用 QnoDDNS 服务密码。



3．域名申请规则：

- 域名最少需为 4 个字，最多 63 个字。
- 域名只能由 a-z(英文小写)、0-9(数字)所组成，且第一个字需为英文字母。
- 域名不得有特殊符号(例如："."；"-"；"_"等等) 。
- 2 Wan 系列产品最多申请 2 个 DDNS 设置。
- 4 Wan 系列产品最多申请 4 个 DDNS 设置。
- 8 Wan 系列产品(含以上)最多申请 4 个 DDNS 设置。



:: 用户数据 ::

姓名	
Email	
序列号	
型号	
Wan数量	

:: 申请规则 ::

1. 如果您申请Qno侠诺科技动态域名服务，代表您同意侠诺科技动态域名服务条款。
2. "用户名称"最少需要4个字，最多63个字(4-63个字)。
3. "用户名称"只能由a-z(英文小写)、0-9(数字)所组成，且第一个字需为英文字母。
4. "用户名称"不得有特殊符号(例如："."；"-"；"_"等等)。(范例)
5. 2 Wan系列产品最多申请2个DDNS设定。
6. 4 Wan系列产品最多申请4个DDNS设定。
7. 8 Wan系列产品(含以上)最多申请4个DDNS设定。

:: Host Name 测试 ::

已输入**0**个字

测试	用户名称：		域名：	qnoddns.org.cn	发送 重设

尚可申请 4 组DDNS

已输入**0**个字

第1组	用户名称：		域名：	qnoddns.org.cn	申请

已输入**0**个字

第2组	用户名称：		域名：	qnoddns.org.cn	申请

已输入**0**个字

第3组	用户名称：		域名：	qnoddns.org.cn	申请

已输入**0**个字

第4组	用户名称：		域名：	qnoddns.org.cn	申请

10.6 广域网接口 MAC 地址设置

有些运营商会要求提供一固定 MAC 地址(网卡物理地址)做为运营商分配 IP 给您的认证使用，此大多适用于 Cable Mode 的用户。若有此需求的话，可使用此功能将提供给运营商的网卡物理地址(MAC 地址：00-xx-xx-xx-xx-xx)填入此项目中， QoS 安全路由器就会以此 MAC 地址作为跟运营商请求 IP 时的认证！

广域网MAC地址设置

接口位置	MAC地址	配置
广域网1	00-17-16-01-35-d0	编辑
广域网2	00-17-16-01-35-d1	编辑

*此为示意图，会因产品线不同，图形会有所差异

选择您要设置的广域网端口，比如"广域网 1"，点击"编辑"进入广域网 1 的端口 MAC 地址设置窗口，使用者可以自行输入提供给运营商的网卡物理地址 MAC，点击此按钮"确认"即会存储刚才所变动的修改设置内容参数，点击此按钮"取消"即会清除刚才所变动的修改设置内容参数，此操作必须于确认存储动作之前才会有效。

目前设备出厂默认的 MAC 位置为 WAN 端的 MAC 地址。

接口位置: WAN1

使用者自订义广域网接口MAC地址：	⦿ 00 - 17 - 16 - 01 - 35 - d0 (默认值: 00-17-16-01-35-d0)
设定与此PC的MAC地址相同：	○ bf-ff-f7-95-00-43

返回 确定 取消

10.7 Inbound Load Balance 对内负载均衡

侠诺防火墙/路由器除了提供效能优异的 Outbound Load Balance 对外负载均衡机制外 现在更加入了 Inbound Load Balance (对内负载均衡) 的功能机制，针对需要平均分配访问内网服务器的外来流量，平均分配在对外的每条线路上，使得频宽使用率能达到最大效益，也能避免因流量分配不均、线路壅塞而导致外网的访问不正常或是中断，更可以只用单一设备就达成内外网流量「双向负载均衡」的需求。

以下我们就按照步骤一一进行来启用与设定 Inbound Load Balance 功能。

※请注意！
目前侠诺的 Inbound Load Balance 功能，部分机种可以先试用一段时间但是有时间限制，若试用结果真的有符合您的网络架构需求，您可以至侠诺官方网站 (www.qno.cn) 进行正式版的产品功能密钥申请，当您完成申请、审核与付费等相关程序，并且成功输入密钥之后，就可不受时间限制使用正式版本。

1.先在「系统工具」=>「许可证密钥」页面把 Inbound Load Balance 试用功能打开。

许可证密钥

当前时间： 2009-11-12 时间服务器地址

许可证密钥内容： [ ]-[ ]-[ ]-[ ]-[ ] 提交

功能名称	试用版	正式版	注册时间	状态与信息
QnoSniff	试用			
Inbound Load Balance	试用			

刷新

开启试用版之后在「状态与讯息」字段会显示试用时间还剩余多少，当剩余剩时间为零 (即试用到齐)，此功能便无法再继续进行试用，除非输入正式版的 License Key (产品功能金钥)。

2.前往「进阶功能配置」的「对内负载均衡」，按下「编辑」开始进行设定。

对内负载均衡

域名	编辑
	编辑
	编辑

3.启用「对内负载均衡」功能

对内负载均衡

☑ 激活对内负载均衡

域名	生存时间	管理者
	7200	@

域名服务器配置

域名服务器	接口位置
.	◉ 广域网1: 192.168.3.143 ○ 广域网2: 0.0.0.0
.	◉ 广域网1: 192.168.3.143 ○ 广域网2: 0.0.0.0

主机记录

主机名称	广域网IP
.	◉ 广域网1: 192.168.3.143 ○ 广域网2: 0.0.0.0
.	◉ 广域网1: 192.168.3.143 ○ 广域网2: 0.0.0.0

别名记录

别名	指向
.	.
.	.

邮件交换记录

主机名	顺序	电邮服务器
.	10	.
.	20	.

*此为示意图，会因产品线不同，图形会有所差异

4.网域名称与主机 IP 对应调整

指定网络架构上层 DNS 服务公司主机/IP 指定动作，以下以 TWNIC 上的设定为例，假设公司目前的网络架构与 IP 如下：

WAN1：ADSL Hinet 210.10.1.1

WAN2：ADSL Seednet 200.1.1.1

Domain Name：abc.com.tw

Name Server(NS)：ns1.abc.com.tw (第一组 NS) /ns2.abc.com.tw (第二组 NS)

前往 TWNIC 网站使用 DNS 主機/IP 修改 (http://rs.twnic.net.tw/index2.html) 如下图所示

DNS 設定/代管

若你不會填表單，請看DNS 設定(DNS模式)範例， DNS 代管(主機模式)範例!

◉ DNS模式 ○ 主機模式

	DNS/主機名稱	IP Address
一	ns1.abc.com.tw	210.10.1.1
二	ns2.abc.com.tw	200.1.1.1
三		
四		
五		

填寫完成請按這裡 填錯了！我要重填

选择 DNS 模式，并且将主机名称的全名填入，对应到预设的 WAN1 与 WAN2 IP 位置，并按下完成，最快全球同步 24 小时即可完成 (在台湾约几分钟就可以测试了)

※请注意！

若您的上层不是 TWNIC 的话，请依照您所注册的运营商去更改主機 /IP 指定动作！若是其它的运营商代管 DNS 的设定，请参照您的运营商所提供的网页画面设定！

5.防火墙/路由器网域名称设定

☑ 激活对内负载均衡

域名	生存时间	管理者
qnoddns.org	5	jay @ qno.com.tw

域名： 依照已先行向网域名称 (Domain Name) 注册单位取得之网域名称，填入此字段 (例如 abc.com.tw)，下方的相关设定项目便会自动将此网域名称带出，不用再输入。

生存时间： 生存时间 (Time To Live 又简称 TTL) 为 DNS 查询间隔时间 (秒)(数值 0~65535)，太长影响更新时间，太短则可能会增加系统负担但是负载均衡结果会较为精准，所以请依您实际的应用状况作调整。

管理者： 为系统管理者的电子邮件信箱，例如 test@abc.com.tw

6.网域名称服务器配置：新增或修改名称服务记录 (NS Record)

NS Record 是网域名称服务器记录，用来指定该网域名称由哪个 DNS 服务器来进行解析。

域名服务器配置

域名服务器	接口位置
.	◉ 广域网1: 192.168.3.143 ○ 广域网2: 0.0.0.0
.	◉ 广域网1: 192.168.3.143 ○ 广域网2: 0.0.0.0

*此为示意图，会因产品线不同，图形会有所差异

域名服务器： 填写已注册的名称服务记录 (NS Record)，例如 ns1、ns2。

接口位置： 指定 WAN IP address 为与名称服务记录相对应的 IP Address，基本上系统会自动带出目前有设定取得的 WAN IP，您可以直接点选，但是也需要确认是否是与上述在 TWNIC 所作的对应设定是相同的 (例如 ns1.abc.com.tw <=> WAN1：210.10.1.1，ns2.abc.com.tw <=> WAN2：200.1.1.1)

7.主机记录：新增或修改主机记录 (A Record)

主机记录

主机名称	广域网IP
.	广域网1: 192.168.3.143 广域网2: 0.0.0.0
.	广域网1: 192.168.3.143 广域网2: 0.0.0.0

*此为示意图，会因产品线不同，图形会有所差异

主机名称： 主机名称记录 (A Record) 需要填写企业规划对外提供服务的主机名称。例如 mail (邮件服务器)、FTP (档案传输服务器)。

广域网 IP： 相对应 A Record 的 IP Address (WAN Port IP)。如果选择多个 WAN IP，表示外网来访的流量将可以平均分配在这数个所选择 WAN IP 所在的频宽与线路上。

8.别名记录：新增或修改别名记录(CN Record)

这种记录允许您将多个名字映射到同一台计算机。通常用于同时提供 WWW 和 MAIL 服务的计算机。

例如，有一台计算机名为“host.mydomain.com”（A 记录）。它同时提供 WWW 和 MAIL 服务，为了便于用户访问服务。可以为该计算机设置两个别名（CNAME）：WWW 和 MAIL。 这两个别名的全称就是“www.mydomain.com”和“mail.mydomain.com”。实际上他们都指向 “host.mydomain.com”。

同样的方法可以用于当您拥有多个域名需要指向同一服务器 IP，此时您就可以将一个域名做 A 记录指向服务器 IP 然后将其他的域名做别名到之前做 A 记录的域名 上，那么当您的服务器 IP 地址变更时您就可以不必麻烦的一个一个域名更改指向了 只需要更改做 A 记录的那个域名其他做别名的那些域名的指向也将自动更改到新的 IP 地址上了。

别名记录

别名	指向
.	.
.	.

别名： 别名记录需要填写列于主机名称 (A Record)，以及需要相对应的别名记录。

指向： 填写已存在于主机记录 (A Record) 的名称。

9.邮件交换记录：新增或修改邮件交换记录 (MX Record)

是邮件交换记录，它指向一个邮件服务器，用于电子邮件系统发邮件时根据 收信人的地址后缀来定位邮件服务器。例如，当 Internet 上的某用户要发一封信给 user@mydomain.com 时，该用户的邮件系统通过 DNS 查找 mydomain.com 这个域名的 MX 记录，如果 MX 记录存在， 用户计算机就将邮件发送到 MX 记录所指定的邮件服务器上

邮件交换记录

主机名	顺序	电邮服务器
.	10	.
.	20	.

主机名： 邮件主机的去除网域部分的主机名称。

顺序： 多部邮件主机之优先次序，以数值小者为优先。

邮件服务器： 填写之别名填写已存在于主机记录(A Record)的主机名，或是外部邮件主机。

将上述设定接设定完成后，按下确定才会使设定值生效，除此之外，还需要进行下述 DNS 服务所使用的相关服务通讯端口的开通做设定。

10.防火墙的访问规则中开放 DNS Query (DNS 访问服务通讯端口)

在防火墙存取规则中，新增一条允许的规则，针对需要进行对内负载均衡的 WAN 口开放 DNS 服务通讯端口。

访问规则设置

管制动作：	允许
服务端口：	DNS[UDP/53~53] 服务端口新增或删除表
日志：	激活
接口位置：	广域网1
来源IP地址：	任何的
目的IP地址：	单独 210 . 10 . 1 . 1

生效时间

管制时间为 所有时间	: 到 : (时间格式:24小时制)
每天	周日 周一 周二 周三 周四 周五 周六

管制动作： 选择「允许」。

通讯端口： 从下拉式选单中选择「 DNS [UDP/53~53] 」。

日志： 依您的需求选择是否需记录相关的 DNS 访问数据，需要的话请选择「启用」。

接口位置： 请选择您要进行负载均衡以及相对应网域名称的 WAN IP 所在的 WAN 口。

来源 IP 地址： 请选择「Any」。

目的 IP 地址： 请选择接口位置与网域名称所注册对应的 WAN IP，以上例来讲就是 210.10.1.1。

生效时间设定： 请选择「所有时间」。

11.在进阶功能的虚拟服务器中，开启 A Record 相对应的内网 IP 与服务通讯端口。

虚拟服务器

服务端口：所有端口 [TCP&UDP/1~65535]
服务端口新增或删除表
内部IP地址：192 . 168 . 8 .
接口位置：ANY
激活：
增加到对应列表
删除选中的项目

通讯端口：	请选择所对应 A Record 服务器所提供服务的通讯端口作开放，例如 Mail 为 SMTP [TCP/25~25]。
内部 IP 地址：	请输入主机名称(A Record) 与主机名称相对应的内部 IP 地址设定，例如 Mail 服务器内部 IP 为 192.168.8.100。
接口位置：	选择主机名称(A Record)与主机名称相对应的 WAN IP 所在 WAN 口界面。
启用：	勾选启用此设定。
加入到对应列表：	将以上设定完成并加入至下方列表之中。

十一、工具程序功能设置

此章节介绍用来管理 QoS 安全路由器以及测试网络联机的工具。

考虑安全的因素，建议修改密码。关于登录密码与路由器时间的设置已经在第五章 5.2 节已经介绍，在此就不做重复介绍了。

11.1 在线联机测试

QoS 安全路由器提供简易的在线测试机制，方便于测试线路质量时使用。此包含 DNS 查询以及 Ping 二种。

○ 域名解析测试　　◉ Ping测试

Ping 此 IP地址或域名：10.10.10.100 [开始]

状态:	测试成功
封包:	4/4 传输, 4/4 接收, 0% 遗失
	最小值 = 1 ms
循环次数:	最大值 = 56 ms
	平均值 = 15 ms

域名解析测试

请于此测试窗口输入您想查询的网域主机位置名称，如 www.abc.com 然后点击开始的按钮开始测试。测试结果会显示于此窗口上。

◉ 域名解析测试　　○ Ping测试

测试域名(www.qno.cn)：www.google.com [开始]

名称:	www.google.com
地址:	72.14.235.99

Ping-数据包传送/接收测试

○ 域名解析测试	◉ Ping测试
Ping 此 IP地址或域名：	10.10.10.100 [开始]
状态:	测试成功
封包:	4/4 传输, 4/4 接收, 0% 遗失
	最小值 = 1 ms
循环次数:	最大值 = 1 ms
	平均值 = 1 ms

此项目为主要提供管理者了解对外联机的实际状况，可以由此功能了解网络上的计算机是否存在！

请于此测试窗口输入您想测试的主机位置 IP，如 168.95.1.1 点击开始的按钮开始测试，测试结果会显示在窗口上。

11.2 系统软件更新

此功能可以让 QoS 安全路由器在 Web 设置窗口中直接做软件升级。请您于升级前先确认软件版本信息。点击"浏览"按钮，选择软件存放文件夹，并于选择欲升级的软件后，点击立即系统软件更新做升级。

注意！

执行软件升级前，请详细阅读窗口中的注意事项。

正在做软件升级当中时，请勿离开此升级窗口，否则会造成 QoS 安全路由器升级失败。

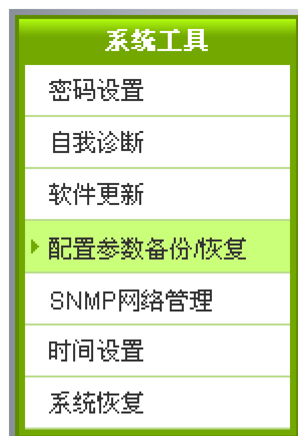
软件更新

[浏覽...]

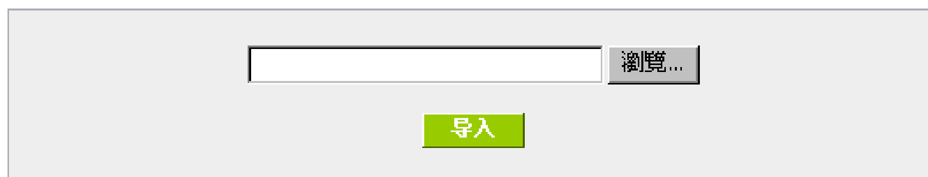
[立即更新]

警告 ： 1. 当您选择前一个版本的软件时，所有的设定都将回复到出厂预设值
2. 软件升级需要一点时间，此时切勿拔除电源或按下Rest按钮
3. 当您在作软件升级时，请勿关闭此画面或中断此联机

11.3 系统设置参数存储



从指定的配置文件恢复



备份目前的配置



从指定的设置文件恢复：

此功能将之前所存储在计算机的备份设置参数内容回存到 QoS 安全路由器中！选择“浏览”至备份参数文件“config.exp”存放数据夹，选择该文件后，点击“导入”按钮做设置文件导入。

备份目前的设置：

此功能为存储网管人员在 QoS 安全路由器的设置参数备份到计算机中，通常做路由器版本升级前，请务必将您现在的路由器设置文件用此功能存储在计算机中！点击存储按钮，选择至备份参数文件“config.exp”存放数据夹位置，点击存储即可。

11.4 网络管理设置(SNMP)

SNMP 为 Simple Network Management Protocol 的缩写，指网络管理通讯协议。此为互联网上使用的一个管理工具。通过此 SNMP 通讯协议，可以让已经具备有网络管理的程序(如 SNMP tools-HP Open View)等网管程序做实时管理之通讯使用。QoS 安全路由器支持标准 SNMP v1/v2c，可以搭配标准 SNMP 网络管理软件来得知目前 QoS 安全路由器上的机器运作情况，以便随时掌握网络信息。

SNMP网络管理

☑ 激活

系统名称：	4_WAN_QVM_Router
联系方式：	
系统地址：	
Get Community Name：	public
Set Community Name：	private
Trap Community Name：	public
Send SNMP Trap to：	

确定 取消

激活：	将 SNMP 功能开启或关闭。系统默认为开启此功能。
系统名称：	设置机器的名称，如 Firewall。
联系方式：	设置机器的管理联系人员名称。
系统地址：	设置机器的目前所在位置。
Get Community Name：	设置一组管理者参数可以取得此机器的项目信息，系统默认“Public”。
Set Community Name：	设置一组管理者参数可以设置此机器的项目信息，系统默认“Private”。
Trap Community Name：	设置一组管理者参数可以传送 Trap 的信息。
Send SNMP Trap 到：	设置一组 IP 地址或是域名名称的接收 Trap 讯号主机。
确定：	点击此按钮“确认”即会存储刚才所变动的修改设置内容参数。
取消：	点击此按钮“取消”即会清除刚才所变动的修改设置内容参数，此操作必须于确认存储动作之前才会有效。

13.5 系统恢复

您可以于此工具中选择 QoS 安全路由器系统重新开机功能，请点击“系统重新启动”的“立即重新激活” 按钮即可重新开机启动。

重新启动

立即重新启动

恢复原出厂设置

立即恢复原出厂设置

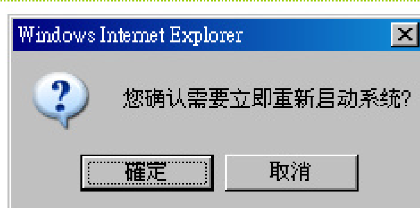
系统重新启动

如图，如果点击系统启动下的“立即重新激活”,会弹出提对话框提示是否重新启动 QoS 安全路由器，确定 QoS 安全路由器就做重新启动操作。

重新启动

立即重新启动

恢复原出厂设置



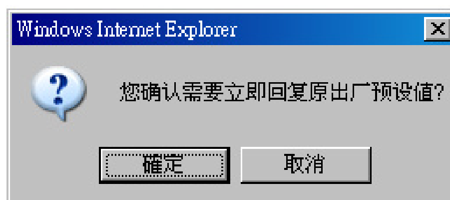
恢复原出厂默认值

若是选择重新恢复“立即重新激活”， 会弹出提对话框提示是否恢复出厂值，确定后 QoS 安全路由器将做恢复出厂值操作。

重新启动

立即重新启动

恢复原出厂设置



我们建议在做版本升级前请先将 QoS 安全路由器现在的设置值存储在计算机当中，等做完版本升级后，使用此功能将机器做出厂值设置以确保机器升级后的稳定运行，然后再将刚才存在计算机的设置直存回 QoS 安全路由器(如何存储路由器的设置数据、及升级完成后如何存回路由器，请参考 13.3 系统设置参数存储说明)。

11.6 High Availability 备援功能

High Availability 备援功能一般是使用于需要架构容错与备援机制的网络环境，通常是透过两个一模一样的设备互作备援，平时由其中一台设备做主要的网络传输，另一台为闲置直到负责主要传输的设备发生网络传输问题时，才马上运做起来使网络传输与相关服务不致中断，也提供网络管理人员更多处理问题的机会与时间，不会因为只有一台设备而导致发生问题时无从下手。

除了提供一般市面规格的 HA 外，侠诺也提供了两台设备能够同时进行网络传输与备援功能的进阶 HA 功能，不用将另外一台设备完全闲置，完全充分利用两台设备的成本效益，并且也不一定必须是要同一种设备，只要都是侠诺且都有支持 HA 的功能设备即可达成。

备援功能

备援功能	◉ 激活	○ 关闭
备份模式:	◉ 硬件备份模式	○ 双机并用备份模式
运作模式:	◉ 主控模式	○ 备份模式
	主控模式与从属模式模式的两个设备设定必须不同	
状态:	正常模式	
备份设备状态:	正常	

確定　取消

备援功能： 激活：表示启用 HA 备援功能。
关闭：表示关闭 HA 备援功能。

备援模式： (1) 硬件备份模式：
为一般规格的备援模式，即两台设备一台负责主要的网络传输，一台完全闲置，直到负责主要传输的设备发生问题，会发出讯息告知闲置的设备立即接手网络传输工作。

(2) 双机并行备援模式：
网络的应用架构是两个设备会同时担负对外连线任务，但仍然会有主要与备援模式分别，主控模式设备在正常状态下为主要 DHCP IP 配发者，备份模式设备在正常状态下则会自动关闭 DHCP 服务器不提供 DHCP 配发 IP 服务，直到主控模式设备发生问题，由备份设备接手所有对外连线任务时，备份模式的设备才会激活 DHCP 服务器提供配发 IP 服务。

以下就以此两个不同模式分别进行说明：

硬件备份模式

备援功能	◉ 激活	○ 关闭
备份模式:	◉ 硬件备份模式	○ 双机并用备份模式
运作模式:	◉ 主控模式	○ 备份模式
	主控模式与从属模式模式的两个设备设定必须不同	
状态:	正常模式	
备份设备状态:	正常	

※选择运作－主控模式： 表示负责所有对外网络连线工作，发生问题时由另一台设备接手备援

状态： 「状态－正常模式」表示一切运作正常。

备份设备状态： 显示目前负责备援的设备状态是否正常，若正常则可以点选链接直接从远程进入负责备援设备进行管理 (另一台必须开启远程管理功能)。
「状态－异常」表示负责备援的另一台设备无法侦测到或不存在，需检查另一台设备目前的状况。

备援功能	◉ 激活	○ 关闭
备份模式:	◉ 硬件备份模式	○ 双机并用备份模式
运作模式:	○ 主控模式	◉ 备份模式
	主控模式与从属模式模式的两个设备设定必须不同	
备份设备的局域网IP:	192 . 168 . 1 . 5	
备份设备的MAC地址:	0 : 0 : 0 : 0 : 0 : 0	
状态:	正常模式	

※选择运作－备份模式：

表示此设备是负责当「主控模式」发生问题时的接手备援任务，所以此设备的广域网 WAN 与局域网 LAN IP 设定必须与「主控模式」设备的设定完全相同，并且此备援设备平时不负责对外的网络传输以及 DHCP 配发 IP 任务。

※若原本的局域网 LAN 是用「主控模式」的 DHCP 配发 IP，那么「备份模式」设备的 DHCP 服务器设定也要与「主控模式」的 DHCP 服务器设定完全相同，这样才能在备援模式真正进行备援动作时，让 DHCP 工作继续正常并且局域网络对外连线不中断。

备份设备的局域网 IP： 请填入「主控模式」设备的 LAN IP 地址。(因为是「被」备援)

备份设备的 MAC 地址： 请填入「主控模式」设备的 MAC 地址。(因为是「被」备援)

状态： 「状态－正常模式」表示目前此备援设备完全闲置，「主控模式」设备工作正常；「状态－备援模式」表示目前此设备已进入接手备援状态负责全部网络传输，「主控模式」设备发生问题，直到 「主控模式」设备正常启动并且发送讯息告知此设备，状态才会恢复成「状态－正常模式」闲置状态。

双机并行备份模式：

备援功能	◉ 激活	○ 关闭
备份模式:	○ 硬件备份模式	◉ 双机并用备份模式
运作模式:	◉ 主控模式 (DHCP激活)	○ 从属模式 (DHCP关闭)
	主控模式与从属模式模式的两个设备设定必须不同	
从属设备的广域网:	☐ 广域网1 ☑ 广域网2 (勾选的广域网本身没有运作)	
从属设备的局域网IP:	192 . 168 . 1 . 5	
备份设备的MAC地址:	0 : 0 : 0 : 0 : 0 : 0	
状态:	正常模式	

*此为示意图，会因产品线不同，图形会有所差异

※运作模式－主控模式： 表示虽然与另一台共同负责对外网络连线工作，但是更多了一个 DHCP 配发 IP 的任务，因为从属模式的设备虽然也有对外连线，但是 DHCP 服务器是不启用的。

从属设备的广域网：(勾选的广域网本身没有运作) 勾选本身没有运作交给另外一台负责的广域网 WAN 连线，譬如总共二条线路，本身是负责 WAN1 的对外连线，WAN2 则交给另外一台负责，则此时就要勾选 WAN2。

从属设备的局域网 IP： 设定另一台从属模式设备所使用的局域网 IP 地址，必须与本身(主控模式)的局域网 IP 不同。

备份设备的 MAC 地址： 设定另一台从属模式设备所使用的局域网 MAC 地址，必须与本身(主控模式)的局域网 IP 不同。

状态： 「状态－正常模式」表示两台设备目前运作正常；「状态－备援模式」表示另一台 (从属模式) 设备发生问题，本机已启用备援功能，接手进行需要备援的广域网连线。

备援功能	◉ 激活	○ 关闭
备份模式:	○ 硬件备份模式	◉ 双机并用备份模式
运作模式:	○ 主控模式 (DHCP激活)	◉ 从属模式 (DHCP关闭)
	主控模式与从属模式模式的两个设备设定必须不同	
从属设备的广域网:	☑ 广域网1 ☐ 广域网2 (勾选的广域网本身没有运作)	
从属设备的局域网IP:	192 . 168 . 1 . 5	
备份设备的MAC地址:	0 : 0 : 0 : 0 : 0 : 0	
状态:	正常模式	

*此为示意图，会因产品线不同，图形会有所差异

※运作模式－从属模式：	表示虽然与另一台共同负责对外网络连线工作，但是本身的 DHCP 服务器功能是关闭的，所以局域网 LAN 的用户要从从属模式设备的广域网 WAN 传输流量，需要在确认从属模式设备的局域网 LAN IP，与「主控模式」设备的局域网 LAN IP 不同，但是要在同一个子网络中。 举例来说，若主控模式设备的 DHCP 服务器 IP 地址为 192.168.1.1 子网掩码 255.255.255.0，则另一台从属模式的设备也必须与 192.168.1.1 在同一个子网络中如 192.168.1.2。
从属设备的广域网： (勾选的广域网本身没有运作)	勾选本身没有运作交给另外一台负责的广域网 WAN 连线，譬如总共二条线路，本身是负责 WAN1 的对外连线，WAN2 则交给另外一台负责，则此时就要勾选 WAN2。
从属设备的局域网 IP：	设定另一台主控模式设备所使用的局域网 IP 地址，必须与本身(从属模式)的局域网 IP 不同。(但是一定要在同一个子网络中)
备份设备的 MAC 地址：	设定另一台主控模式设备所使用的局域网 MAC 地址，必须与本身(从属模式)的局域网 IP 不同。
状态：	「状态－正常模式」表示两台设备目前运作正常；「状态－备援模式」表示另一台 (主控模式) 设备发生问题，本机已启用备援功能，接手进行需要备援的广域网连线，并启用 DHCP 服务器功能。

11.7 产品功能许可证密钥

Qno 侠诺系列防火墙 / 路由器产品，会有一些功能的「启用」或是「正式版」(非试用版)，会需要申请与购买许可证密钥才能够进行使用。例如 QnoSniff (侠诺神捕)、Inbound Load Balance (对内负载均衡) 等。

许可证密钥

当前时间： 2009-11-10 时间服务器地址

许可证密钥内容： [ ] - [ ] - [ ] - [ ] - [ ] 提交

功能名称	试用版	正式版	注册时间	状态与信息
QnoSniff	V			剩馀: 4 天 19 时
Inbound Load Balance	V			剩馀: 8 天 20 时

刷新

当前时间： 在输入正式版许可证密钥 (License Key) 时，系统自动检查目前的时间是否正确，并且密钥是否仍然在有效的时间内，所以强烈建议您在试用与输入正式版密钥时，先检查并更新至目前最新且正确的时间，以避免在使用功能时产生问题。

许可证密钥内容： 输入您所申请与购买的正式版产品密钥内容，一般是数十个英文与数字的组合，输入之后按下「提交」，系统会检查该把产品密钥是否合法正确，如果是合法正确即可开始使用该功能正式版，下方该功能的正式版栏位也会打勾。

功能名称： 显示加值的功能列表，若出厂默认值在试用版栏位没有「试用」按钮，表示该功能无法进行试用，或是该类功能是属于如 QnoSoftKey 之类的支持隧道数量。

试用版 / 正式版： 可以进行试用的功能项目在出厂默认值时，会在试用版的栏位中显示「试用」按钮，按下按钮后就可以试用该功能一段时间。

正式版栏位在您申请并且成功输入密钥、认证成功后，会在该栏位打勾表示该功能项目已经成为正式版，不用受到试用版天数的限制。

注册时间： 显示产品功能密钥成功输入并注册的时间。

状态与信息： 显示目前试用版剩余的试用天数，或是 QnoSoftKey 等目前系统所支持的隧道数量。

刷新： 重新更新目前系统功能的状态与时间。

十二、日志功能设置

日志功能纪录 QoS 安全路由器的运行数据，并以可读的方式呈现再设置窗口上提供给您作为参考。您可以依据需求检视这些信息。

12.1 系统日志

QoS 安全路由器的日志记录提供三种设置：系统日志， 电子邮件通知，以及选择日志的类别。

发送到日志服务器

☑ 激活

主机名称：	0.0.0.0	(正确网域名称或IP地址)

发送到电子邮箱

☑ 激活

电邮服务器：		(正确网域名称或IP地址)
电子邮件：		

发送数量：	50	笔
发送间隔时间：	10	分钟

立即发送到电子邮箱

系统日志配置

告警日志		
☐ Syn Flooding	☐ IP Spoofing	☐ Win Nuke
☐ Ping Of Death	☑ 登入认证错误	

一般日志		
☑ 系统错误信息	☐ 被阻挡的管制条例	☐ 允许通过的管制条例
☑ 系统配置变更	☑ 认证登入	

查看系统日志 出去NAT记录 进入NAT记录 清除日志

系统日志

激活传送到日志服务器: 若是勾选此选项的话，传送系统日志功能将被开启。

系统日志服务器主机名称: QoS 安全路由器 提供了外部系统日志服务器收集系统信息功能。系统日志为一项工业标准通讯协议，于网络上动态撷取有关的系统信息。QoS 安全路由器的系统日志 提供了包含动作中的联机来源位置与目的位置，服务编号以及状态。输入您要接收系统日志的服务器名称或是 IP 地址于"系统日志服务器"的空格字段内。

电邮告警功能(未来支持)

激活传送到电子邮箱: 若是勾选此选项的话，电子邮件告警将会被开启。

电邮服务器: 请输入电子邮件服务器的名称或是 IP 地址，如 mail.abc.com。请注意，您必须有权限经由所填入的电子邮件服务器寄送日志电子邮件，否则此日志电子邮件将无法被寄出。

电邮地址: 此为设置日志收件人电子邮件信箱，例如 abc@mail.abc.com

传送日志数量: 自定日志数量，系统默认为 50 条。 当到达此数量时， QoS 安全路由器将会自动 Mail 传送日志。

传送区隔时间: 自定传送日志间隔时间，系统默认为 10 分钟。 当到达此时间时， QoS 安全路由器将会自动 Mail 传送此日志。
QoS 安全路由器将会自动判别当数量或是间隔时间哪一个参数先到达，就 Mail 传送日志信息给管理者。

立即传送到电子邮箱: 使用管理者可以直接按此按钮传送日志。

系统日志设置

系统日志配置

告警日志		
☐ Syn Flooding	☐ IP Spoofing	☐ Win Nuke
☐ Ping Of Death	☑ 登入认证错误	

一般日志		
☑ 系统错误信息	☐ 被阻挡的管制条例	☐ 允许通过的管制条例
☑ 系统配置变更	☑ 认证登入	

查看系统日志 | 出去NAT记录 | 进入NAT记录 | 清除日志

QoS 安全路由器 提供了包含以下的告警内容信息，您只要打勾点选即可包含在日志信息中。

Syn Flooding： 即在短时间内传送大量的 syn 数据包，造成系统记录联机的内存溢满。

IP Spoofing： 通过数据包监听程序来拦截网络上所传送数据，并在读取后藉由程序修改原发送端地址，进入原目的端的系统内，存取资源。

Win Nuke： 通过侵入或设陷阱的方式将木马程序送入对方服务器中。

Ping of Death： 通过传送来产生超过 IP 协议所能够允许的最大数据包，造成系统宕机。

登录认证错误： 当系统发现有企图登录 QoS 安全路由器的入侵者时，就会将信息传到系统日志中。

一般系统日志信息

QoS 安全路由器 提供了包含以下的一般性内容信息，您只要打勾点选即可。系统错误信息，被阻挡的管制条例，允许通过的管制条例，认证登录，系统设置变更。

系统错误信息： 提供系统中各种错误给系统日志。例如：不正确的设置或是功能异常状况发生。

被阻挡的管制条例： 当有用户试图进行存取规则中不允许的规则时，此信息会传送到系统日志中。

允许通过的管制条例： 当用户进行存取规则所允许的规则时，此信息会传送到系统日志中。

系统设置变更： 当系统的设置值改变时，此信息回传送到系统日志中。

认证登录： 每一个成功登录系统的 IP 地址都会传送并记录到系统日志中。

以下有四个有关查询日志的按钮，分别叙述如下：

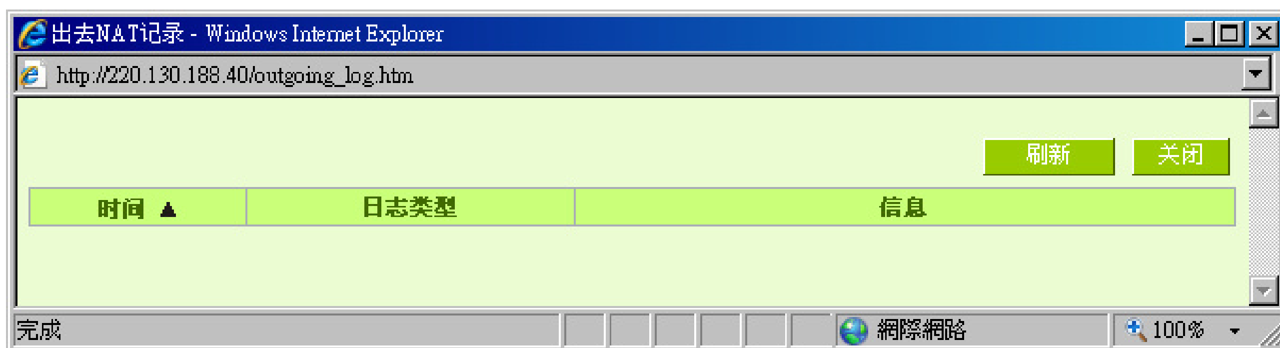
查看系统日志：

此为查看系统日志使用，其信息内容可以从下拉式选单中分类读取，包含全部日志， 系统日志，防火墙日志。选择“刷新”按钮可以刷新日志显示窗口，“清除”按钮可以清除所有日志记录。如下图所示：



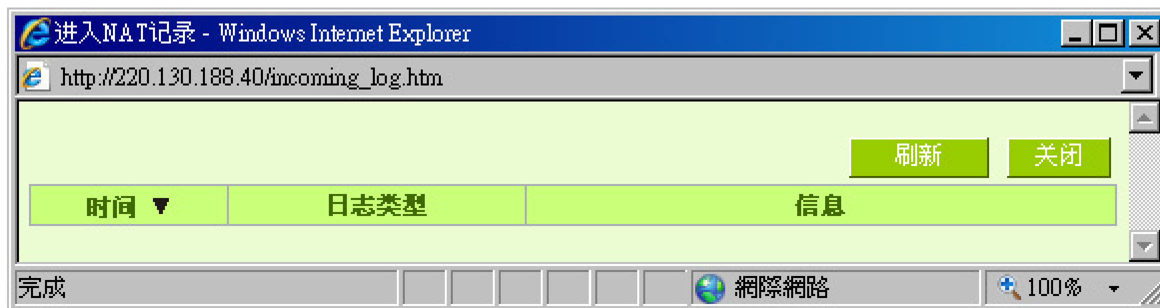
<u>出去 **NAT** 记录：</u>

查看内部 PC 出互联网的系统数据包日志，此日志包含内部网络地址，目的地地址以及所使用的通讯服务端口号、类型等信息。



<u>进入 **NAT** 记录：</u>

查看外部进入 QoS 安全路由器的系统数据包日志，此日志内含外部来源网络地址， 目的地地址与通讯端口号等信息。



<u>清除日志：</u>

此按钮为清除所有目前 QoS 安全路由器的日志相关信息。

12.2 系统状态实时监控

QoS 安全路由器的系统状态实时监控管理功能可以提供系统目前的运行信息，包含局域或广域端口名称，目前端口联机状态，IP 地址，网络实体位置(MAC 地址)，子网掩码，默认网关，域名解析服务器(DNS)，网络侦测，收到的数据包数量，传送的数据包数量，全部的进出数据包数量统计，收到的数据包 Byte 流量统计，传送的数据包 Byte 流量统计，全部进出的数据包 Byte 流量统计，收到的错误数据包统计以及端口丢弃的数据包统计，会话数，新联机数，上传带宽使用率，下载带宽使用率等信息。

系统状态

下一页

端口：	广域网1接口	广域网2接口	USB 1	局域网
机器名称：	eth1	eth2	ppp3000	eth0
目前端口连线状态：	联机	激活	关闭	---
IP 地址：	192.168.3.108	0.0.0.0	---	192.168.1.1
MAC 地址设定：	00-17-16-03-26-CE	00-17-16-03-26-CF	---	00-17-16-03-26-CD
子网掩码：	255.255.255.0	0.0.0.0	---	255.255.255.0
预设网关 IP 地址：	192.168.3.1	0.0.0.0	---	---
域名解析服务地址：	192.168.3.10	0.0.0.0	---	---
线路侦测机制：	测试成功	测试失败	---	---
收到的网络包数量：	1758	0	---	2972
传送的网络包数量：	1085	0	---	3877
全部的网络包数量：	2843	0	---	6849
收到的网络包 Byte 数量：	261279	0	---	423041
传送的网络包 Byte 数量：	155810	0	---	2456424
全部的网络包 Byte 数量：	417089	0	---	2879465
接收 Bytes/秒：	300	0	---	2156
传送 Bytes/秒：	0	0	---	30789
收到的错误网络包统计：	0	0	---	0
端口丢弃的网络包统计：	0	0	---	0
联机状态（session)：	0	0	---	---
新联机数/秒：	0	0	---	---
上传带宽使用率：	0	0	---	---
下载带宽使用率：	0	0	---	---

*此为示意图，会因产品线不同，图形会有所差异

12.3 流量统计

QoS 安全路由器提供六种显示流量统计的信息，来提供管理者对于流量有更好的管理与控制。

流量统计

☑ 激活

网络流量统计方式： 依下载流量的会话

目的IP地址	通讯协议	目的端口	来源IP地址	来源端口	bytes/sec	%

刷新

依上传流量的 IP 地址：

在此图表中显示了从外进入内网流量的来源端的 IP 地址， 每秒有多少 byte 与所占的百分比。

网络流量统计方式： 依上传流量的IP地址

来源IP地址	bytes/sec	%
10.10.10.100	1395	100

刷新

依下载流量的 IP 地址：

在此图表中显示了从内网出去流量的来源端的 IP 地址， 每秒有多少 byte 与所占的百分比。

网络流量统计方式： 依下载流量的IP地址

来源IP地址	bytes/sec	%
10.10.10.100	8737	100

刷新

依上传流量的端口：

在此图表中显示了以网络的服务端口来分类进入内网使用流量统计(每秒)byte 与百分比。

网络流量统计方式： 依上传流量的端口

通讯协议	目的端口	bytes/sec	%
TCP	443	2862	98
UDP	8000	30	1
TCP	1863	4	0

刷新

依下载流量的端口：

在此图表中显示了以网络的服务端口来分类从内网出去的使用流量统计(每秒)byte 与百分比。

网络流量统计方式： 依下载流量的端口

通讯协议	目的端口	bytes/sec	%
TCP	2082	160	50
TCP	443	70	22
TCP	2083	52	16
TCP	1863	29	9

刷新

依上传流量的会话：

在此图表中显示了从广域网络进来的(Dest. IP)地址所联机的局域网络的 IP(Source IP)位置所使用的服务端口(Dest.Port)还有现在使用流量(bytes/sec)与百分比。

网络流量统计方式： 依上传流量的会话

来源IP地址	通讯协议	来源端口	目的IP地址	目的端口	bytes/sec	%
10.10.10.100	TCP	3802	59.124.180.50	443	30	68
10.10.10.100	UDP	4000	58.251.60.87	8000	5	12
10.10.10.100	TCP	3803	59.124.180.50	443	4	9

刷新

依下载流量的会话：

在此图表中显示了从局域网络的 IP(Source IP)地址对外联机的目的地位置(Dest. IP)IP 及所使用的服务端口(Dest.Port)还有现在使用流量(bytes/sec)与百分比。

网络流量统计方式： 依下载流量的会话

目的IP地址	通讯协议	目的端口	来源IP地址	来源端口	bytes/sec	%
10.10.10.100	TCP	3979	65.55.15.244	80	72	37
10.10.10.100	TCP	3964	122.116.228.7	443	39	20
10.10.10.100	TCP	3980	207.46.26.26	1863	36	19
10.10.10.100	UDP	1056	168.95.1.1	53	29	15
10.10.10.100	TCP	3328	207.46.107.46	1863	12	6

刷新

12.4 会话数统计(未来支持)

会话数统计功能用来记录内网的会话数量，可以列出目前有对外流量、会话的内网用户 (计算機)，并且显示该用户会话数的统计与会话内容。

会话数统计

☑ 激活

目前有流里的PC	总会话数
1	9

局域网计算机数据排序依照 IP地址由小到大　　跳到 1 / 1 页　　每页显示 10 笔

IP地址	主机名称	会话数
192.168.8.100	QnoPM01	9
192.168.8.102	8_WAN_SVR_Router	0

刷新

激活： 启用会话数统计功能，此功能启用后会影响整个路由器部分的处理效能，所以当勾选启用时，系统会提醒您会因此产生效能上的影响。

目前有流量的 PC： 显示目前有对外会话并且有网络流量的用户计算机数量，如果用户计算机没有开机或是没有对外会话网际网，可能就不会计算在统计数量之中。

局域网计算机数据排序依照： 选择数据清单的显示排序是以「IP 地址由小到大」、「IP 地址由大到小」
、「会话数由小到大」、「会话数由大到小」那一种排序基准做显示。

跳到___/___页：
每页显示___笔 选择每页显示几笔数据，并且可以直接以下拉式选单前往其它页面。

数据列表

IP 地址： 显示有对外流量用户计算器的 IP 地址。
并且可以点选 IP 链接，显示目前会话的统计内容与细节 (如下图)：

IP/端口流量监控

☑ 激活

查询方式依 IP地址 IP地址 : 192 . 168 . 8 . 100 搜索

总会话数	TCP总会话数	UDP总会话数	下载带宽 Bytes/Sec	上传带宽 Bytes/Sec
6	6	0	8	4

来源IP地址	通讯协议	来源端口	接口位置	目的IP地址	目的端口	下载带宽 Bytes/Sec	上传带宽 Bytes/Sec
192.168.8.100	TCP	50360	WAN1	192.168.3.10	1339	0	0
192.168.8.100	TCP	50361	WAN1	192.168.3.10	443	0	0
192.168.8.100	TCP	50362	WAN1	192.168.3.10	443	8	4
192.168.8.100	TCP	50364	WAN1	192.168.3.10	443	0	0
192.168.8.100	TCP	50365	WAN1	192.168.3.10	443	0	0
192.168.8.100	TCP	50371	WAN1	65.54.48.134	1863	0	0

刷新

主机名称：	显示有对外流量用户的计算机名称，无法解析出来时会显示空白。
会话数：	显示目前有对外流量用户计算器的总会话数量。
刷新：	按下按钮可以更新至目前最新的数据内容与清单。

12.5 特定 IP 及端口状态

QoS 安全路由器提供网管人员可以针对某一 IP 或某一特定端口去查询此 IP 去访问的目的地址，或是有哪些人使用这个服务端口。其目的可以方便找出某些需要认证的网站无法走多 WAN 端口而必须走单一个 WAN 端口，网管人员可以查询出此目的地的 IP 做协议绑定来解决此登录问题。另外，若想查询何人在使用 BT 或 P2P 软件，也可选择 Port 做使用者查询。

IP/端口流量监控

☑ 激活

查询方式依 IP地址 IP地址：0 . 0 . 0 . 0 查询

来源IP地址	通讯协议	来源端口	接口位置	目的IP地址	目的端口	下载带宽 Bytes/Sec	上传带宽 Bytes/Sec

刷新

特定 IP 状态：

直接在 IP 地址里填入您想要查询的 IP 地址，就可以显示出此 IP 对外联机的所有目的地及端口号。

查询方式依 IP地址 IP地址：10 . 10 . 10 . 100 查询

来源IP地址	通讯协议	来源端口	接口位置	目的IP地址	目的端口	下载带宽 Bytes/Sec	上传带宽 Bytes/Sec
10.10.10.100	TCP	3328	WAN2	207.46.107.46	1863	0	0
10.10.10.100	TCP	3351	WAN2	59.124.180.50	443	4	22
10.10.10.100	TCP	3352	WAN2	59.124.180.50	443	18	4
10.10.10.100	UDP	4000	WAN2	58.251.60.87	8000	70	39
10.10.10.100	TCP	3802	WAN2	59.124.180.50	443	0	0
10.10.10.100	TCP	3803	WAN2	59.124.180.50	443	0	0
10.10.10.100	UDP	6001	WAN2	58.251.62.71	8000	0	0
10.10.10.100	TCP	3964	WAN2	122.116.228.7	443	40	25
10.10.10.100	TCP	3977	WAN2	59.124.180.50	443	0	0
10.10.10.100	TCP	3978	WAN2	59.124.180.50	443	0	0
10.10.10.100	TCP	3980	WAN2	207.46.26.26	1863	4	20
10.10.10.100	UDP	1056	WAN2	168.95.1.1	53	0	0
10.10.10.100	TCP	3981	WAN2	208.50.79.27	80	0	0
10.10.10.100	UDP	6007	WAN2	210.22.23.177	8000	0	0

刷新

特定端口状态：

直接在端口里填入您想要查询的端口号，就可以显示出此端口现在有哪些 IP 正在使用。

查询方式依 服务端口 服务端口：80 查询

来源IP地址	通讯协议	来源端口	接口位置	目的IP地址	目的端口	下载带宽 Bytes/Sec	上传带宽 Bytes/Sec
60.248.180.226	TCP	2110	WAN2	220.130.188.40	80	471	885
60.248.180.226	TCP	2111	WAN2	220.130.188.40	80	52	57
60.248.180.226	TCP	2112	WAN2	220.130.188.40	80	99	873
60.248.180.226	TCP	2113	WAN2	220.130.188.40	80	52	57
60.248.180.226	TCP	2114	WAN2	220.130.188.40	80	0	0

刷新

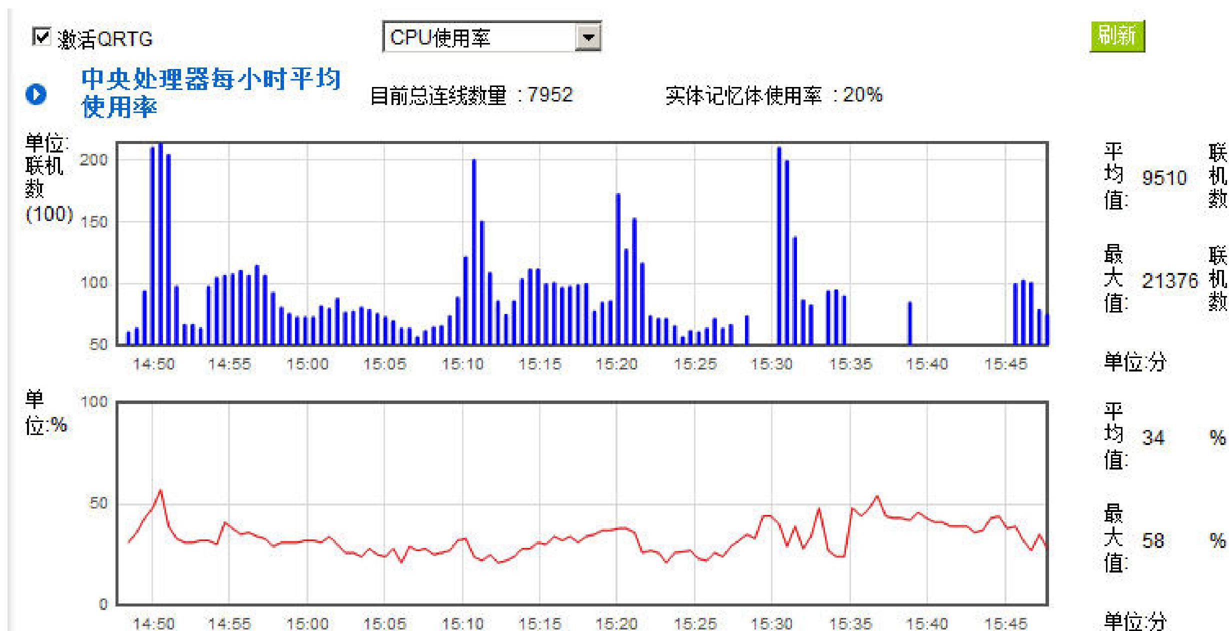
12.6 QRTG (Qno Router Traffic Grapher)

QRTG 是利用动态的图形表示与简单的统计数值，显示目前 Qno 防火墙/路由器系统的工作状态，包括 CPU 使用率、实体内存 (Memory) 使用率、连线数量 (Session) 以及每个广域网的流量 (WAN Traffic)。

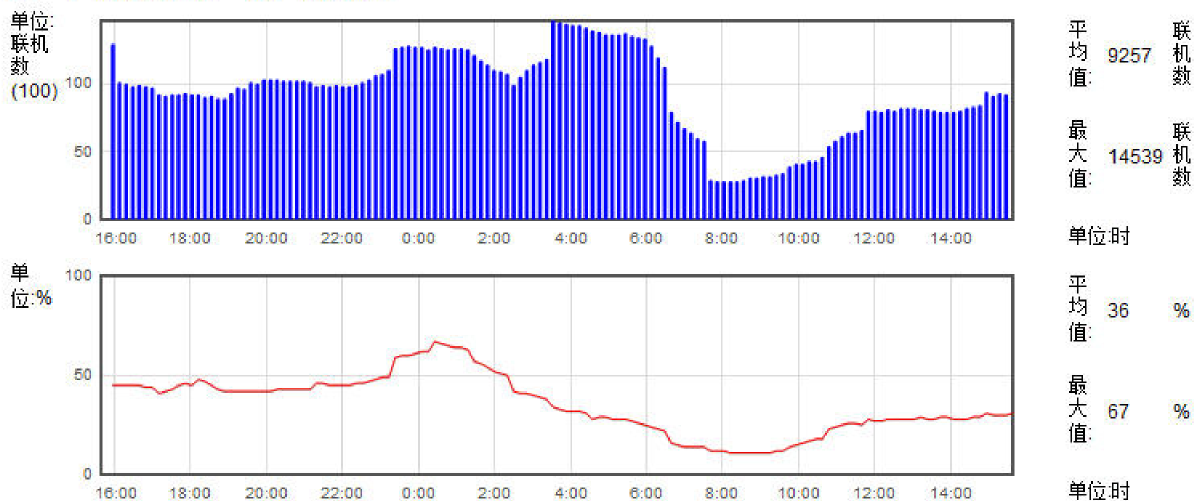
激活 QRTG：QRTG 在系统出厂默认值是不启动的，当您要激活 QRTG 功能时，系统会跳出警告讯息提醒您此功能的激活可能会影响路由器的使用效能。激活之后，您可以透过下拉式选单选择以下项目的目前的状态与统计数值、图形，按下「刷新」按钮会重新更新统计数据与图形内容至最新时间的资料。

一、CPU 使用率 / 连线数量统计 (如下图)

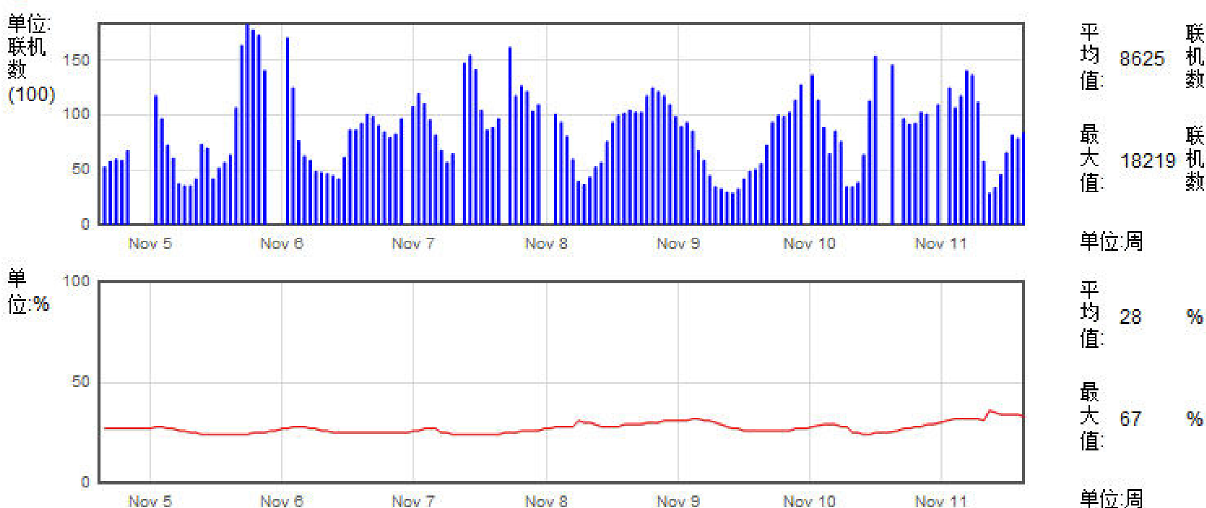
(1) CPU、连线数每小时使用率图形 / 平均值 / 最大值。
(2) CPU、连线数每一天平均使用率图形 / 平均值 / 最大值。
(3) CPU、连线数每一周平均使用率图形 / 平均值 / 最大值。



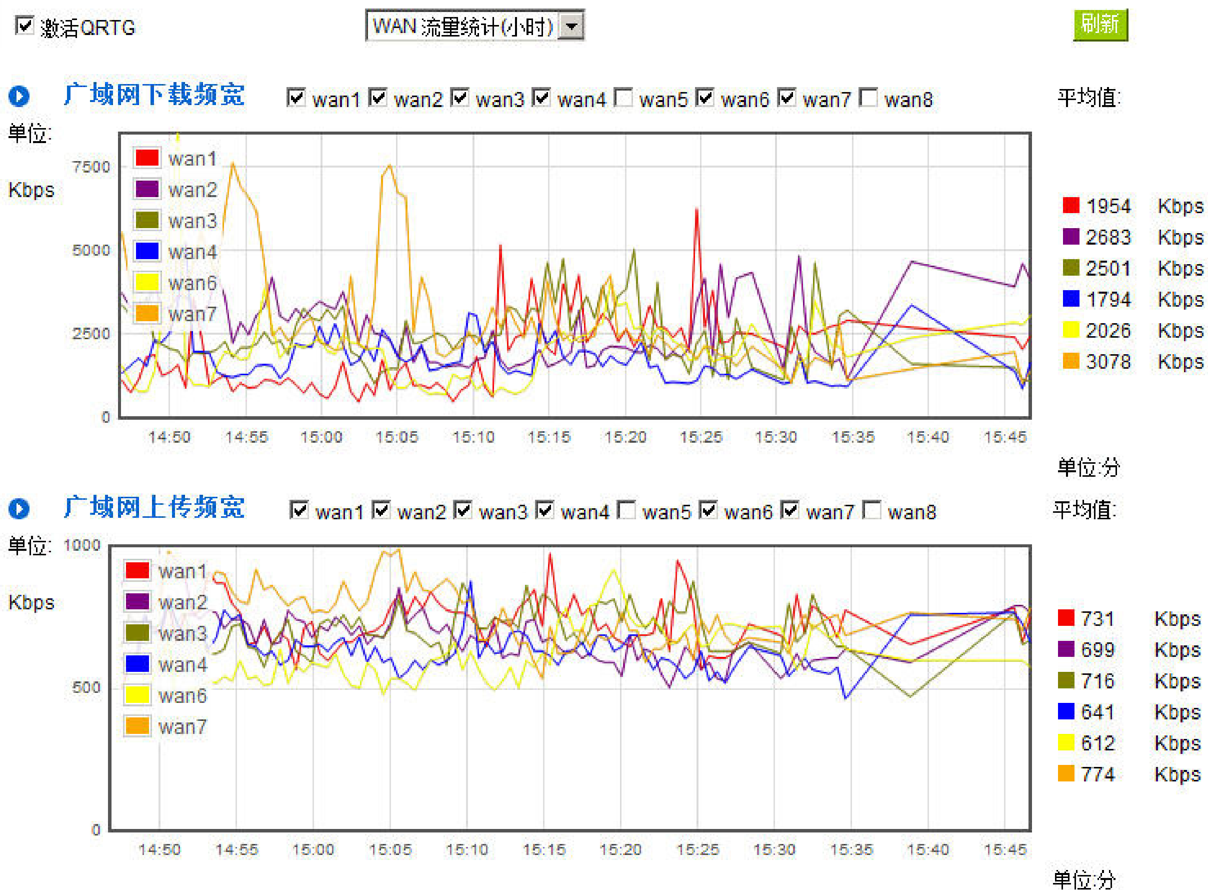
中央处理器每一天平均使用率



中央处理器每一周平均使用率



二、每个广域网「每小时」流量统计图形与平均值 (上传流量与下载流量)(如下图)



*此为示意图，会因产品线不同，图形会有所差异

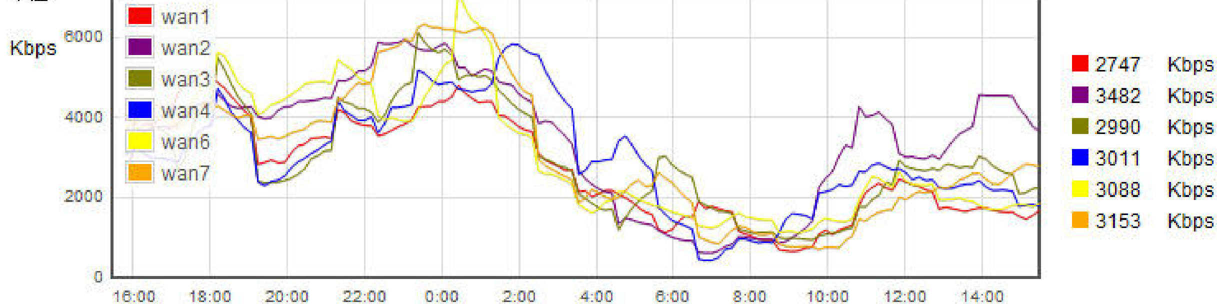
三、每个广域网「每一天」流量统计图形与平均值 (上传流量与下载流量)(如下图)

☑ 激活QRTG   WAN 流量统计(一天)   刷新

广域网下载频宽 ☑ wan1 ☑ wan2 ☑ wan3 ☑ wan4 ☐ wan5 ☑ wan6 ☑ wan7 ☐ wan8   平均值:

单位:

Kbps



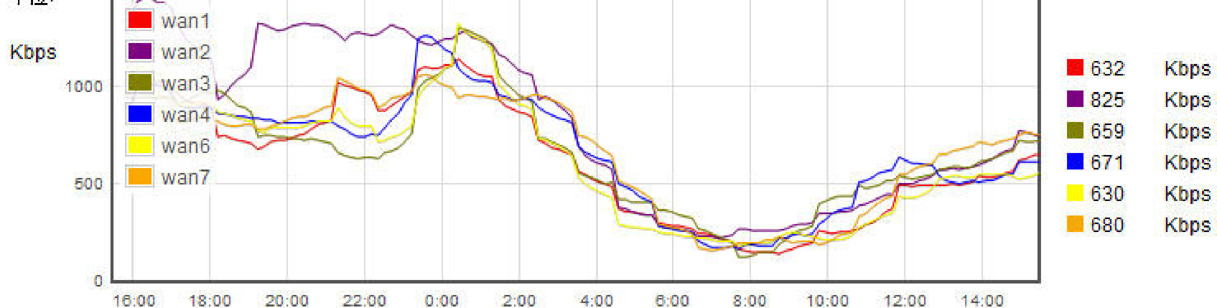
2747	Kbps
3482	Kbps
2990	Kbps
3011	Kbps
3088	Kbps
3153	Kbps

单位:时

广域网上传频宽 ☑ wan1 ☑ wan2 ☑ wan3 ☑ wan4 ☐ wan5 ☑ wan6 ☑ wan7 ☐ wan8   平均值:

单位:

Kbps

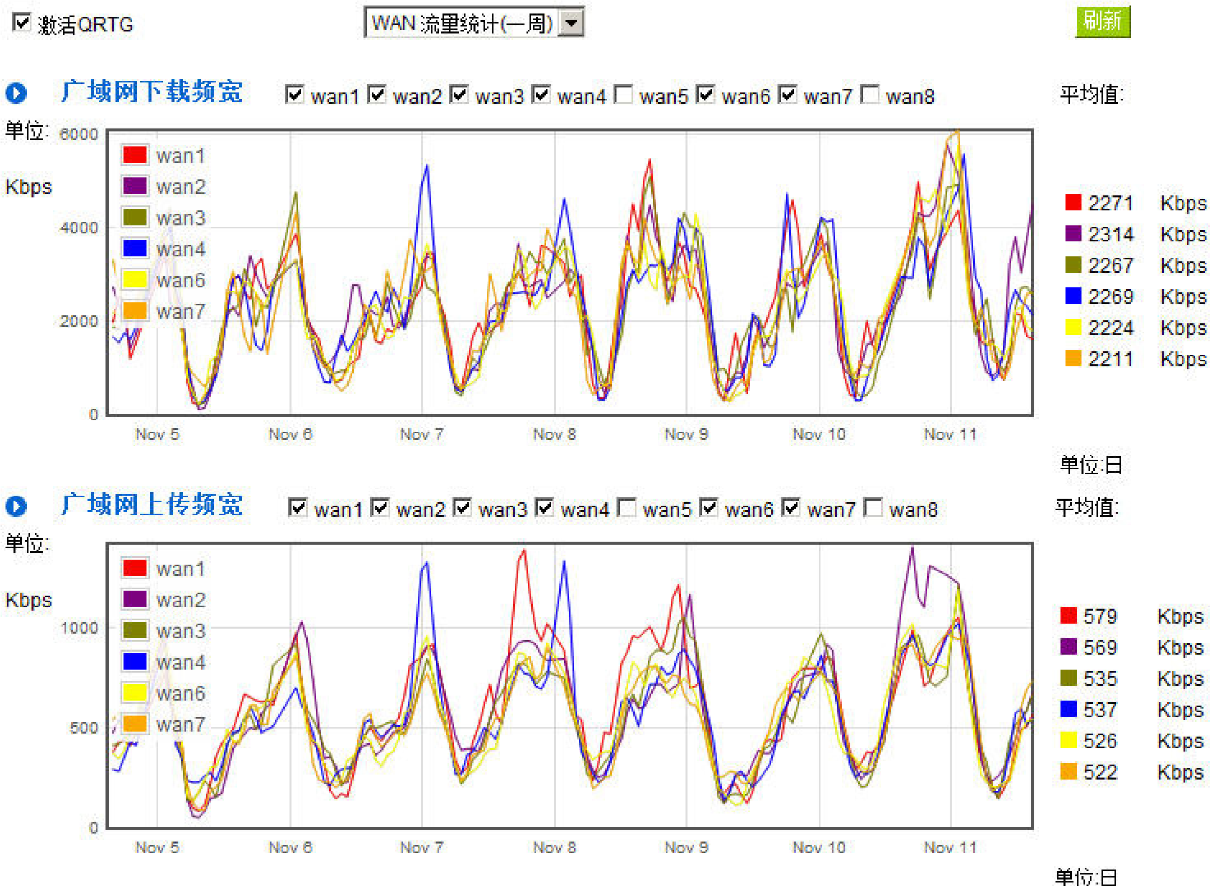


632	Kbps
825	Kbps
659	Kbps
671	Kbps
630	Kbps
680	Kbps

单位:时

*此为示意图，会因产品线不同，图形会有所差异

四、每个广域网「每一周」流量统计图形与平均值 (上传流量与下载流量)(如下图)



*此为示意图，会因产品线不同，图形会有所差异

十六、注销

QoS 安全路由器的网页窗口右上方有一个注销的按钮，此按钮为结束管理 QoS 安全路由器并关闭此管理窗口。若您下次想再进入 QoS 安全路由器管理窗口时，您必须重复登录 QoS 安全路由器管理窗口的步骤，并输入管理者的使用名称与密码。



附录一、设置界面及使用手册章节对照

本章主要通过表格的形式把每个章节具体对照 QoS 安全路由器 Web 管理页面的链接与界面对照显示，进一步方便用户快速的设置路由器，同时更加了解 QoS 安全路由器的工作能力。

QoS 安全路由器整体界面栏目次序图如下。



一级栏目	二级栏目	对应章节
首页		五、确定设备规格、状态显示以及登录密码和时间的设置 5.1 首页显示
网络联线设置		六、进行广域网络连线设置
	网络设置	6.1 网络设置
	流量管理	6.2 多 WAN 设置
	协议绑定	6.2 多 WAN 设置
	虚拟邊境	6.2 多 WAN 设置
USB 设置		請上 Qno 官網下載使用手冊。 http://www.Qno.com.tw

游戏端口加速		8.3 硬件加速服务
QoS 带宽管理		八、QoS 带宽管理功能
	带宽管理	8.1 带宽设置(QoS)
	会话数管理	8.2 会话数管控
IP/DHCP 设置		七、内部局域网络设置
	DHCP 设置	7.3 DHCP 发放 IP 服务器
	DHCP 状态	7.4 DHCP 状态显示
	IP 与 MAC 绑定	7.5 IP 及 MAC 地址绑定
	IP 群组管理	7.6 IP 群组管理
防火墙设置		九、防火墙设置
	基本设置	9.1 基本设置
	访问规则设置	9.2 访问规则设置
	内容过滤	9.3 网页内容管制
高级设置		十、其它进阶高级功能设置
	DMZ/虚拟服务器	10.1 DMZ / 虚拟服务主机
	UPnP 通讯协议	10.2 UPnP- Universal Plug and Play
	路由通讯协议	10.3 路由通讯协议
	一对一 NAT	10.4 一对一 NAT
	动态域名服务	10.5 DDNS-动态域名解析
	广域网 MAC 地址设置	10.6 广域网接口 MAC 地址设置
	对内负载均衡	10.7 对内负载均衡
系统工具		十一、工具程序功能设置/五、确定设备规格、状态显示以及登录密码和时间的设置
	密码设置	5.2 登录密码和时间的设置
	自我诊断	11.1 在线联机测试
	软件更新	11.2 系统软件更新
	设置参数备份/恢复	11.3 系统设置参数存储
	SNMP 网路管理	11.4 网络管理设置(SNMP)
	时间设置	5.2 登录密码和时间的设置
	系统恢复	11.5 系统恢复
	备援功能	11.6 High Availability 备援功能
	产品功能许可证密钥	11.7 产品功能许可证密钥
端口管理		七、内部局域网络设置

	端口设置	7.1 网络端口管理设置
	端口状态即时显示	7.2 网络端口状态实时显示
日志		十四、日志功能设置
	系统日志	12.1 系统日志
	系统状态	12.2 系统状态实时监控
	流量统计	12.3 流量统计
	会话数统计	12.4 会话数统计
	IP/端口流量监控	12.5 特定 IP 及端口状态
	QRTG	12.6 QRTG

附录三：常见问题解决

（1） QQ 容易掉线问题

a). 检查 QQ 版本是否为 2006 版，经过 QQ 官方确认使用珊瑚版或是传美版掉线严重。

b). 2 条以上的线路，必须作协议绑定，让 QQ 走固定广域网。绑定 QQ(UDP8000~8004)走固定的广域网参照下图协议绑定设置：

协议绑定

服务端口： QQ [UDP/8000~8004]
服务端口新增或删除表
来源IP地址 0 . 0 . 0 . 0 到 0
目的IP地址： 0 . 0 . 0 . 0 到
0 . 0 . 0 . 0
接口位置： 广域网1
激活： ☑
上移 更新特殊应用软件 下移
QQ [UDP/8000~8004]->0.0.0.0~0(0.0.0.0~0.0.0.0)广域网1
删除选中的项目 新增

c).保证带宽给 QQ 端口，依照网吧或企业内部实际带宽评估 QoS 所需要设置的最小值与最大值，下图为 10M 光纤保证给 QQ 的方式，上下传都必须设置。

QoS带宽管理

控制类型： ⦿ 带宽控制 ○ 优先级

接口位置： ☑ 广域网1 ☑ 广域网2

服务端口： QQ [UDP/8000~8004]

服务端口新增或删除表

IP地址 : 0 . 0 . 0 . 0 到 0

目的： 上传

保证带宽： 200 Kbit/sec 最大可用带宽： 2000 Kbit/sec

带宽分配方式： ○ 此范围每一IP地址独享此设定带宽. ⦿ 此范围所有IP地址共享此设定带宽.

激活： ☑

上移 更新特殊应用软件 下移

QQ [UDP/8000~8004]->0.0.0.0~0(上传)=>200~2000Kbit/sec->WAN1, 2

删除选中的项目 新增

（2）阻挡基本 BT 种子下载方式

若您想要封锁 BT 种子，不让用户下载，您可以直接在 "防火墙设置" => "内容过滤" 选择 "设定禁止访问的域名" 后将 "网页内容过滤(关键字)" 打入".torrent"这样就可以防止用户下载种子。

○ 设定允许访问的域名
◉ 设定禁止访问的域名

禁止访问的域名

☐ 激活

网页内容过滤(关键字)

☑ 激活

关键字：.torrent (仅支持英文关键字)

管制所有IP地址 : 0 . 0 . 0 . 0 到 0

更新字符串

.torrent->管制所有IP地址

删除选中的项目 新增

（3） 冲击波及蠕虫病毒的防制

由于近来还是发生有许多用户局域网中冲击波及蠕虫病毒造成局域网访问互联网很慢及联机数(Session)大量增加造成 QoS 安全路由器大量处理，以下将指导您封锁此些病毒相应端口以达到防制目的。

a.增加此 TCP135-139， UDP135-139 还有 TCP445 端口:

服务名称：

通讯协议： TCP

端口范围： 到

增加到对应列表

HTTPS [TCP/443~443]
HTTPS Secondary [TCP/8443~8443]
TFTP [UDP/69~69]
IMAP [TCP/143~143]
NNTP [TCP/119~119]
POP3 [TCP/110~110]
SNMP [UDP/161~161]
SMTP [TCP/25~25]
TELNET [TCP/23~23]
TELNET Secondary [TCP/8023~8023]
TELNETSSL [TCP/992~992]
DHCP [UDP/67~67]
L2TP [UDP/1701~1701]
PPTP [TCP/1723~1723]
IPSec [UDP/500~500]
TCP [TCP/135~139]
UDP [UDP/135~139]
TCP [TCP/445~445]

删除选中的项目

确定 取消 关闭

b.用防火墙里面的"存取规则"功能将设置好的此三组端口封锁:

访问规则设置

管制动作：	禁止
服务端口：	TCP [TCP/135~139] 服务端口新增或删除表
日志：	激活
接口位置：	任何的
来源IP地址：	任何的
目的IP地址：	任何的

用同样的方法添加好 UDP[UDP135~139]以及 TCP[445~445]端口。

c.将这三组的优先级至于最高:

跳到 1 / 2 页 每页显示 5 笔 下一页>>

优先级	激活	管制动作	服务端口	接口位置	来源IP地址	目的IP地址	管制时间	日	编辑	删除
1	☑	关闭	TCP [445]	*	任何的	任何的	所有时间		编辑	
2	☑	关闭	UDP [135]	*	任何的	任何的	所有时间		编辑	
3	☑	关闭	TCP [135]	*	任何的	任何的	所有时间		编辑	
	☑	允许	所有端口 [*]	局域网	任何的	任何的	所有时间			
	☑	关闭	所有端口 [*]	广域网1	任何的	任何的	所有时间			

添加新规则 恢复出厂默认值

（4） 阻止 QQLive 视频直播设置

QQLive 视频直播软件是一种流媒体点播软件，最近好多客户都在头痛一个同样的问题，当局域网有多个用户使用 QQLive 视频直播软件，占用了比较大的带宽，造成 QoS 安全路由器的负担过重，使得 QoS 安全路由器反应迟钝或瘫痪，如果我们能够封锁 QQLive 的服务器登录过程就可以解决这样的问题，下面就这个问题来结合 Qno 产品的相关功能提出相关的解决方案，来进行 QoS 安全路由器设置。

a). 进入路由器 Web 管理页面，再进入"防火墙设置"的"访问存取规则设置"。

访问规则设置

管制动作：	禁止	
服务端口：	所有端口 [TCP&UDP/1~65535]	服务端口新增或删除表
日志：	关闭	
接口位置：	任何的	
来源IP地址：	任何的	
目的IP地址：	单独	58 . 60 . 11 . 145

生效时间

管制时间为 所有时间	: 到 : (时间格式:24小时制)
每天	周日 周一 周二 周三 周四 周五 周六

返回 确定 取消

b). 再点击"增加新的管制规则"，进入"访问存取规则设置"页面，在"存取服务规则设置"中的"管制动作"选项中选择"禁止"，再在"服务器端口" 选择"所有端口[TCP&UDP/1~65535]"，选择"来源接口"为"任何的"，"来源 IP 地址"选择"任何的"(有相关需求的用户可以选择"单独"或"范围" 阻止单个 IP 或者一段 IP 的 QQLive 的的登录)，再在"目的 IP 地址"选择"单独"填入 QQLive 服务器的 IP 地址"121.14.75.115"（QQLive 服务器的 IP 地址不止一个，后面需要重复添加)，最后在"时间管制设置"的"此存取规则选择"所有时间"，"确定"后进入下一步骤。

c). 重复以上的操作在只替换"目的 IP 地址"里分别填入以下 IP 地址：

121.14.75.115

60.28.234.117

60.28.235.119

222.28.155.17

可封锁的 QQ Live 版本：QQ Live 2008 (7.0.4017.0)

测试日期:2008-07-29

重复添加后可以看到相关 QQLive 的服务器的连接被封锁，点击确认完成对阻止 QQLive 视频直播设置，此方案是在 QQLive3.1 的版本下测试并完成阻挡的。

附录三：Qno 技术支持资讯

更多有关侠诺产品技术资讯，除了可以登录侠诺宽带讨论区、叁照 FTP 服务器的相关实例；或是进一步联系侠诺各经销商技术部门、或侠诺大陆技术中心取得相关协助。

网上讨论区及 FTP 服务器：

讨论区：http://www.Qno.cn/forum

各大经销商服务联系方式：

用户可以登录网站先上服务页面查询各大经销联系方法：

http://www.Qno.cn/web/where_buy.asp

技术中心：

电邮：QnoFAE@qno.com.tw